(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 May 2001 (17.05.2001)

PCT

(10) International Publication Number
WO 01/35570 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US00/30427

(22) International Filing Date:
6 November 2000 (06.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/434,516 5 November 1999 (05.11.1999) US

(71) Applicant: NETCHARGE.COM, INC. [US/US]; Suite 202A, 2201 East Camelback Road, Phoenix, AZ 85016 (US).

(72) Inventors: SMITH, Greg, E.; 326 NW 15 Street, Oklahoma City, OK 73103 (US). SCHLINKERT, Leo, R.; 30 Goodwives River Road, Darien, CT 06820-5918 (US).

(74) Agent: COULSON, Lesley, L.; Morgan, Lewis & Bockius LLP, 1800 M Street N.W., Washington, DC 20036-5869 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/35570 A1

(54) Title: PAYMENT METHOD AND SYSTEM FOR ONLINE COMMERCE

(57) Abstract: The system of the present invention which creates a payment system for online commerce is implemented through client software on the computers of the system participants and a central transaction administration system. Each client software component interacts with the client software of other system participants and with the central transaction administration system. The transaction administration system receives transaction requests from each party to a transaction and compares the information received from each party to ensure that the transaction information received from each party matches, thereby authenticating the transaction.

PAYMENT METHOD AND SYSTEM FOR ONLINE COMMERCE

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to conducting commerce utilizing the Internet, and more particularly to a payment system that utilizes a transaction administration system to process, authorize and match purchase requests to merchants, verify merchant fulfillment of the purchase request and execute the associated credit or debit payment from the purchasing party's account to the merchant.

Description of Related Art

The significant increase in Internet access and use has resulted in a new method of conducting business – electronic commerce. In a typical electronic commerce transaction, a buyer purchases goods or services from a merchant that has established a way for prospective customers to access, order, receive or pay for that merchant's goods and services utilizing the Internet. These transactions are currently performed using conventional credit cards, debit cards, money orders or cash-on-delivery services of shipping companies.

Credit cards and debit cards have been used in commerce for many years. In a typical conventional credit card transaction, the consumer physically authenticates himself in the presence of the merchant by presenting his card and agrees to the terms of the transaction by signing a purchase slip and simultaneously taking physical possession of the purchased goods. The merchant can usually electronically confirm that the purchase amount is within the card's credit limit.

After the transaction, the merchant delivers the purchase slip to his bank (the "Acquiring Bank") for payment. Using an association, such as Visa or MasterCard, the Acquiring Bank delivers the purchase slip to the bank that issued the credit card (the "Issuing Bank"), which credits the Acquiring Bank. The purchase slip may be delivered physically or electronically.

The Issuing Bank typically uses the ground mail system to deliver statements, confirm transactions, and receive payments from cardholders.

Credit and debit cards are currently being used in Internet sales transactions as a form of payment. However, in an online transaction, the customer cannot physically present the card, sign a purchase slip, and take delivery of the goods. Credit and debit cards lose many of their key attributes of providing expedient, reliable and secure

payments. As a result of this inability, issuing banks and card associations impose onerous fees and expensive charge back obligations on the merchant. These expose the merchant to fraud by cardholders and thiefs who obtain possession of the card account nubers.

Additionally, because of the risk of identity theft, the uncertainty surrounding the fulfillment of a transaction, and general privacy concerns, many users are reluctant to transmit account information over the Internet.

Furthermore, for micropayment transactions, where the transaction amount is small, it may not be financially practical for a seller to use a conventional card as a method of payment for the transaction.

The Internet also represents a significant and growing source of merchant fraud against the existing credit and debit card system, in part because of the rapid formation of merchants with a limited operating history. One of the advantages of Internet commerce is that the Internet is capable of connecting customers and merchants, or even two private individuals, in transactions where the parties do not know each other and will have no association in the future. However, these anonymous transactions create new types of transaction risks for all parties to an electronic transaction. The risks created by these anonymous transactions cannot be addressed with the existing debit or credit card systems.

Another risk that is unique to the Internet is with the intellectual property that is acquired and delivered via the Internet, such as software, games or music files. Such intellectual property is exposed to effectively unlimited copying and use in violation of the rights of the owner of the intellectual property. The current payment systems have no reliable method or procedure that can link the purchaser of intellectual property with the use of said intellectual property, or even a method verifying that the purchaser in fact received a working copy of the subject intellectual property. Because the owner or licensor of intellectual property may have difficulty verifying that the purchaser received the purchased or licensed intellectual property, the owner is currently limited in his ability to enforce payment by the purchaser and to protect from outright theft.

Another security issue is the potential for credit card and debit card fraud. Unlike a physical transaction, the merchant cannot ask the buyer for identification in an online transaction. Anyone that acquires a valid credit card account number can

potentially use it to make purchases. There is also a potential for merchant fraud. Once the merchant has the credit card account number, he can potentially misuse it by overcharging the buyer, not delivering the goods ordered after receiving payment, or giving the account number to another. Additionally, there is the risk of interception by third parties, as the credit or debit card account number and other personal information is electronically transmitted during the transaction processing.

The current response to such issues is to use electronic certificates and encryption. However, such methods generally only address the card holder side of the security issue, and may have limited effectiveness due to technical constraints. More importantly, encryption only helps ensure that the message was not altered – it does not authenticate the sender of the message, nor does it ensure the accuracy of the original message.

Another problem that arises with the current payment system is the difficulty and expense of "unwinding" a transaction. When a customer returns a purchased item, the return transaction is usually handled as a separate transaction from the original purchase transaction. This additional processing, which is usually manual, is very expensive, especially for small purchases. In some cases, it may cost a merchant more to process a merchandise return than the merchandise itself is worth.

Therefore there is a need for an expedient, secure, and reliable method of conducting commerce utilizing the Internet.

SUMMARY OF THE INVENTION

The present invention has been made in view of the above circumstances and solves the problems of current payment systems by creating an on-line payment system that verifies the authenticity of the transaction parties, verifies that the transaction details are correct, facilitates the verification of delivery of the goods and services, provides increased protection to owners of intellectual property conducting business on the Internet, prevents the misappropriation of personal information, prevents Internet identity theft through credit or debit card information, and reduces the cost of unwinding an electronic commerce transaction in a manner that does not constrain or diminish the cost-reducing impact of the Internet on commerce.

One object of the present invention is to provide an on-line payment system that uses electronic real-time connections to match, authenticate, and confirm all the components of a transaction between all the parties involved in the transaction that

does not require the use of traditional physical credit or debit cards or the transmission of card account numbers to make purchases.

Another object of the present invention is to provide a transaction administration system for confirming and authorizing transactions by receiving the terms of the transaction from a first transaction party, receiving the terms of the transaction from a second transaction party and comparing the terms of the transaction received from the first transaction party with the terms of the transaction received from the second transaction party to determine whether the terms match.

A further object of the present invention is to provide a method for merchants to obtain authorization of an electronic transaction by providing transaction information to the buyer, receiving a transaction key from the buyer, transmitting the transaction key to the transaction administrator and receiving a purchase authorization from the transaction administrator.

A further object of the present invention is to provide a transaction administration system for confirming delivery of purchases by receiving the terms of the delivery from a transaction party, receiving the confirmation of the delivery from a delivery agent and comparing the terms of the delivery received from the transaction party with the delivery confirmation to determine whether the terms match.

A further object of the invention is to provide a method of identifying a transaction party through his client software.

Additional objects and advantages of the invention will be set forth in part in the description that follows, and in part will be obvious from the description, or may be learned by practice of the invention. The objects and advantages of the invention will be realized and attained by means of the elements and combinations particularly pointed out in the appended claims.

To achieve these and other objects, and in accordance with the purposes of the invention, as embodied and broadly described herein, one aspect of the invention includes a method of authenticating an electronic transaction between a plurality of transaction parties by a transaction administrator. This method comprises receiving the terms of the transaction from a first transaction party; receiving the terms of the transaction from a second transaction party; comparing the terms of the transaction received from the first transaction party with the terms of the transaction received

from the second transaction party to determine whether the terms match; and if the terms match, validating the transaction.

A further aspect of the invention includes a method for a seller to obtain authorization of an electronic transaction. This method comprises providing transaction information including a seller identifier to a buyer; receiving a transaction key from the buyer; transmitting the transaction key to a transaction administrator; and receiving an authorization from the transaction administrator.

Another aspect of the invention includes a method of authorizing an electronic transaction between a plurality of transaction participants by a transaction administrator. This method comprises providing transaction information by a first transaction party to the transaction administrator; generating a transaction key by the transaction administrator and providing the transaction key from the transaction administrator to the first transaction party; providing the transaction key from the first transaction party to a second transaction party; providing the transaction key from a second transaction party to the transaction administrator for validation; and validating the transaction by the transaction administrator.

Another aspect of the invention includes a method of authorizing an electronic transaction between a plurality of transaction participants by a transaction administrator. This method comprises providing transaction information by a first transaction party to the transaction administrator; generating a transaction key by the transaction administrator and providing the transaction key from the transaction administrator to the first transaction party; providing the transaction key from the first transaction party to a second transaction party; providing the transaction key from a second transaction party to the first transaction party; providing the transaction key from the first transaction party to the transaction administrator for validation; and validating the transaction by the transaction administrator.

Another aspect of the invention includes a method of authenticating the delivery of goods between a plurality of transaction parties. This method comprises providing a transaction administration system for confirming delivery of purchases; receiving the terms of the delivery from a transaction party; receiving the confirmation of the delivery from a delivery agent; and comparing the terms of the delivery received from the transaction party with the delivery confirmation to determine whether the terms match.

Another aspect of the invention includes a method of authenticating a transaction between a plurality of transaction parties. This method comprises requesting a transaction from a second transaction party by a first transaction party; providing transaction information to the transaction administrator by the second transaction party; requesting the first transaction party to confirm the transaction request; providing confirmation to the transaction administrator by the first transaction party; comparing the confirmation with stored confirmation data for the first transaction party; and validating the transaction by the transaction administrator.

Another aspect of the invention includes a method of authenticating a transaction between a plurality of transaction parties. This method comprises requesting a transaction by a first transaction party from a second transaction party; providing transaction information to the transaction administrator from the second transaction party; providing a transaction number to the second transaction party by the transaction administrator; communicating the transaction number to the first transaction party by the second transaction party; confirming the transaction by the first transaction party contacting the transaction administrator and communicating the transaction number; comparing the confirmation provided by the first transaction party with the stored transaction number; and validating the transaction by the transaction administrator.

Another aspect of the present invention includes a method of unwinding a transaction between a buyer and a seller each having an account with a transaction administrator. This method comprises requesting a return transaction from the seller; receiving a return transaction number; returning goods to a delivery agent; delivering the return goods to the seller by the delivery agent; and crediting the buyer's account and debiting the merchant's account by the transaction administrator upon the seller's receipt of the return goods.

Another aspect of the present invention includes a method of verifying the electronic purchase and delivery of intellectual property between a plurality of transaction parties, where a first transaction party requests to purchase downloadable intellectual property from a second transaction party by a transaction administrator. This method comprises providing transaction information to a transaction administrator; generating and providing a transaction key and a private delivery key to the first transaction party by the transaction administrator; providing the transaction

key to the second transaction party from the first transaction party; providing the transaction key to the transaction administrator by the second transaction party; validating the transaction by comparing the received transaction key with the one generated; if the transaction is validated, providing a public delivery key to the second transaction party; providing the intellectual property to the first transaction party encrypted with the private delivery key; and decrypting the intellectual property by the first transaction party.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention that together with the description serve to explain the principles of the invention.

In the drawings:

Fig. 1 illustrates the enrollment process for buyers, merchants, shipping agents, and issuing banks.

Fig. 2 illustrates the relationships of the transaction parties for a typical transaction in the present invention.

Fig. 3 illustrates software components of the system of the present invention.

Fig. 4 illustrates the connectivity of the system of the present invention.

Fig. 5 is a flowchart illustrating the basic transaction authentication process of the system of the present invention.

Fig. 6A-B illustrate embodiments of the transaction authentication process.

Fig. 7A-B illustrate the data flow for embodiments of the transaction authentication process.

Fig. 8 is a flowchart illustrating the process for authentication from a remote terminal.

Fig. 9 is a flowchart illustrating the process for an off-line transaction from a telephone.

Fig. 10 illustrates the Order Delivery Confirmation Service process.

Fig. 11 illustrates the Online Delivery process.

Fig. 12 illustrates the periodic payment process.

DETAILED DESCRIPTION

Reference will now be made in detail to exemplary embodiments of the present invention, examples of which are illustrated in the accompanying drawings. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like components.

A key issue for the growth of electronic commerce over the Internet is the ability to be able to order goods and services without the fear of privacy invasion or credit or debit card fraud. A number of encryption methods and other methods have been used to address this issue; however, these methods only reduce certain risks. Moreover, they do not attempt to address authentication or original message validity. Therefore electronic transactions are still vulnerable to theft or fraud.

The present invention solves the problems of conventional card based electronic commerce transactions by creating an on-line payment system that does not use traditional physical credit or debit cards, signatures, or account numbers. The system of the present invention is implemented through client software on the computers of the system participants and a central transaction administration system. Each client software component interacts with the client software of one or more other system participants and with the central transaction administration system. The transaction administration system receives transaction requests other parties to a transaction and simultaneously compares the information received from each other to ensure that the transaction information received from each party matches, thereby authenticating the transaction.

Preferably, in a typical transaction handled by the system of the present invention, the first party to the transaction is a buyer, the second party to the transaction is a merchant, and the transaction request is a request from the buyer to purchase goods or services from the merchant charging the purchase price to the buyer's account with a financial institution affiliated with the transaction administration system. The transaction administration system compares the terms of the transaction as the buyer knows them to the terms of the transaction as the merchant knows them, to ensure that all terms match. The terms in a buyer-merchant transaction may include the buyer's identity, the merchant's identity, item identifiers, prices and quantities, payment mechanisms, and delivery instructions. If the terms of the transaction as known by the buyer match the terms as known by the merchant,

then the transaction administration system may authenticate the transaction. When the merchant receives authorization from the transaction administration system, he ships or downloads the purchased goods or information to the buyer.

Every transaction party that participates in the system has a unique and private identifier. The identifier is assigned to a party through his client software. The actual party to a transaction does not even need to know what his identifier is, as the client software on his computer automatically identifies that party to the system. The identifiers are preferably embedded in the client software, and not made known to the users. The identifiers are used by the transaction administrator in the authentication matching process. Only the transaction administration system can tell who a party is through an identifier. Because a system identifier cannot be altered, duplicated or stolen, the risk of fraud is virtually eliminated. Additional security can be achieved by using a password or PIN in conjunction with the private identifier.

In a preferred embodiment, when a buyer makes a purchase request, the client software on his computer sends his unique identifier to the client software on the merchant's system. The buyer's identifier becomes one of the transaction terms that the merchant "knows" for purposes of the authentication matching that takes place later. The merchant does not actually know who the buyer is, but rather the client software on the merchant's system receives the buyer's identifier as part of the process. The client software on the merchant's system sends the merchant's unique identifier to the buyer, adding to the terms of the transaction that the buyer "knows" through the buyer's client software.

When the transaction administration system compares transaction terms, the purchase will only be approved if all of the terms, including the party identifiers, match. If all of the terms match, the transaction administration system generates and returns a transaction key to the buyer. To complete the process, the buyer transmits the transaction key to the merchant. The merchant gets final approval for the purchase by transmitting the transaction key back to the transaction administration system. The transaction administration system validates the transaction by matching the transaction key that was sent back by the merchant with the one that it generated when it performed the first match. The merchant does not ship or download the purchased goods, or perform the purchased services, until he receives a validation confirmation from the transaction administration system.

By going through this process, there is a high level of assurance that the buyer is buying said goods or services, and that the merchant has agreed to the terms. The process of matching ensures that there is no transaction misunderstanding and therefore little possibility of transaction fraud.

Matching can be applied to the delivery of the goods or services as well as the sale of the goods or services. By electronically connecting the delivery agent, the transaction administrator can confirm actual delivery of goods and services.

By using an electronic matching network, the system of the present invention allows all users, includes individuals, to act as buyers and sellers. Since both parties are electronically linked to a network, either can act as buyer or seller. This enables individuals to act as sellers, allowing for person to person electronic commerce.

In the system of the present invention, a credit or debit card account number is not required. Instead, the transaction parties are directly linked with the transaction administration system. The accounts are established when the buyer and merchant register or enroll with the transaction administration system. The system identifies the transaction parties through the client software on each party's computer.

Although the system of the present invention is described in terms of credit or debit cards, it should be understood that the concepts of the system of the present invention can be variously and appropriately applied and combined with many types of financial services and products. For example, Demand Deposit Accounts, Direct Debit Accounts, Lines of Credit, Securities Accounts, Mutual Fund Accounts, and Stored Value Accounts can be advantageously combined with or compliment the system of the present invention. Many types of financial transactions, such as installment loans, secured debt accounts or revolving debt accounts, can be implemented by the system of the present invention.

The system of the present invention implements a Transaction Administration system to process purchase requests over a public network, such as the Internet. A Transaction Administrator (TA), working with affiliated financial institutions, may act as a clearinghouse, cash recipient, and/or payment disburser to the actual parties of an online transaction. The TA validates the transaction by comparing the terms of the transaction that one transaction party knows with the terms of the transaction that another transaction party knows. Parties to the transaction may include buyers, merchants and shipping agents. The transaction term matching that the TA performs

can apply to sales as well as delivery transactions. The TA will validate the transaction only if all the terms match.

The matching process virtually eliminates transaction and settlement risks. Neither party can claim to have not entered into the transaction, nor that delivery was not completed. Additionally, the terms of sale and delivery are unambiguously settled by the TA, thereby defining the contract between the parties.

In the system of the present invention, the parties to an electronic transaction register or enroll with the system before any transactions take place. The enrollment process identifies a party to the system, and provides each party with the appropriate software to enable that party to participate in the system. Fig. 1A-1D illustrate the preferred four types of parties to the system and the process of enrolling for each party.

A preferred "Merchant" is an organization selling goods or services via the Internet. For a merchant to participate in the system of the present invention, he must become an Authorized Merchant with the system. As shown at step **110** in Fig. 1A, an online merchant can request to participate in the system, or be asked to participate in the system. If the merchant decides to participate, he signs an agreement with the TA agreeing to use the system as a form of payment. The agreement defines the transaction terms for the merchant, comparable to the merchant who accepts VISA or MasterCard. The TA provides the Authorized Merchant with Merchant software in step **112**. This Merchant software may include Application Program Interfaces (APIs) and Applications that the Authorized Merchant must integrate into its Website and order fulfillment system in order to participate in the system, at step **114**. The APIs typically manage communications with the TA and with existing Merchant software programs. The Merchant software can be electronically transmitted to the Merchant, or it can be delivered via CD-ROM or the like. The Merchant software preferably establishes a unique identifier to identify the Merchant's system to the TA at step **116**. This Merchant ID is used throughout the system to identify the Merchant to the TA.

A preferred "Issuing Bank" is a financial institution subject to federal and/or state banking laws that is authorized to offer consumer credit and demand deposit accounts in the jurisdictions in which it operates. Any Issuing Bank that participates in the system already has the infrastructure and technology to offer debit and credit transaction in real-time.

As shown at step **120** in Fig. 1B, a financial institution can request to participate in the system, or be asked to participate in the system. If the financial Institution decides to participate, it may sign a "franchise" agreement with the TA. The TA preferably provides Issuing Bank software to the financial institution in step **122**. This Issuing Bank software may include Application Program Interfaces (APIs) and Web Connection Modules that the financial institution integrates into its systems, at step **124**. This software can be electronically transmitted to the financial institution, or it can be delivered via CD-ROM or the like. Once the software is integrated, the financial institution becomes an Issuing Bank within the system.

A preferred "Shipping Agent" can be any type of shipping company or service. For a shipping agent to participate in the system of the present invention, he must become an "Participating Shipper". A Participating Shipper will utilize the system's tracking software and collect required signatures from package recipients as part of the Order Delivery Confirmation service. As shown at step **130** in Fig. 1C, a shipping agent can request to participate in the system, or be asked to participate in the system. If the shipping agent decides to participate, he signs an agreement with the TA. The TA provides Shipper software to the shipping agent in step **132**. This Shipper software may include APIs and Applications that the shipping agent integrates into its system in order to participate in the system, at step **134**. This software can be electronically transmitted to the shipping agent, or it can be delivered via CD-ROM or the like. Once the shipping agent has integrated the Shipper software, he becomes a Participating Shipper.

A preferred "Account Holder" can be an individual or corporation that establishes a credit/debit relationship with an Issuing Bank. An Account Holder can set up subaccounts to manage the transactions of employees or family members. The subaccounts can be linked to purchase order systems or secure email approval notices to an authorizing party.

To become an Account Holder in the preferred system of the present invention, a person or organization must request to participate in the system, as shown at step **140** in Fig. 1D. When the Account Holder decides to participate, he signs an agreement with the TA agreeing to terms of usage. The TA provides Account Holder software to the Account Holder in step **142**. The Account Holder software typically includes Internet browser plug-ins or applets. The Account Holder installs the

Account Holder software at step **144**. This software can be electronically transmitted to the Account Holder, or it can be delivered via CD-ROM or the like.

The Account Holder software creates a unique identifier to identify the Account Holder's computer to the TA at step **146**. It is through the Account Holder software that the system identifies the Account Holder. There are a number of methods that can be used to uniquely identify the computer or device through the Account Holder client software. The identifier may be determined through a fixed spot on the computer's hard drive, through the CPU's identifier, or through a secret token embedded in the software, for example. The Account Holder does not know his identifier, and cannot give it away. The transaction administration system may periodically establish new Account Holder identifiers to further ensure security. Additional security may be achieved by using a password or Personal Identification Number (PIN) in conjunction with the private ID established by the Account Holder client software.

The Account Holder software is typically a browser plug-in that works with publicly available Internet browsers, such as Netscape Navigator and Microsoft Explorer. In addition, instead of a browser plug-in, the Account Holder software may be a Wireless Application Protocol designed to work with the Operating Systems on handheld wireless devices, such as Palm OS, Go OS, and Mac OS, or with digital wireless telephones.

The Account Holder client software may have built-in links to Quicken and Microsoft Money, so that transaction information can be populated into these applications. With the Account Holder client software, the Account Holder may review online payment histories, and the like.

The Account Holder client software may also be customized so that it can block purchases by amount, type of goods, or Merchant. This is an important feature for Account Holders who wish set up subaccounts for family members or employees.

A preferred relationship between the participating entities of the present invention are shown in Fig. 2 and will now be explained. Merchant **290** is an organization selling goods or services via the Internet that has registered with the Transaction Administrator (TA) **250** to become an Authorized Merchant. To participate in the system, Merchant **290** has integrated the Merchant Software into its e-commerce Website and order fulfillment system. This enables purchasers to choose

the system of the present invention as the method of payment when making purchases from the Merchant's Website. Account Holder **280** preferably has a standard Merchant-Client relationship with Merchant **290**, ordering retail products and/or services from Merchant **290**.

Each participating Merchant **290** preferably establishes an account at a Merchant Bank **220** that also participates in the system. Merchant Bank **220** is responsible for making payments to the Merchant **290** on receipt of valid credit events. As indicated by the dashed lines, TA **250** can also act as a Merchant Bank. Merchants may electronically present payment events to TA **250** or a Merchant Bank **220** for payment.

In a preferred embodiment, Merchant Bank **220** or TA **250** has an account at each Issuing Bank **210**. Merchant Bank **220** sweeps on a regular basis to credit Merchant accounts, collecting payments due as directed by TA **250**, or TA **250** may act as a Merchant Bank, and process disbursements from Issuing Bank **210** to Merchant **290**.

The preferred Account Holder arrangements, Issuing banks **210** establish credit/debit relationships with the system's registered Account Holders **280**. Issuing Bank **210** establishes the account and provides funds availability to the Account Holder **280**. Issuing Bank **210** sends statements to Account Holder **280** just like a traditional credit card or debit card issuing bank.

TA **250** preferably maintains control of discount points, coupon distribution and discounts from Merchants to Account Holders. TA **250** may provide customer service for the software and technology for Account Holders for the Issuing Bank.

Merchant **290** may also establish an account with Shipper **260**. In the preferred embodiment, Account Holder **280** receives purchases goods via delivery from Shipper **260**. In charge-on-delivery transactions, the Account Holder's account is debited upon signing/receipt of the goods. Shipper **260** transmits the required information to TA **250**. Shipper **260** also has an account with Merchant **290**.

TA **250** provides the real-time transaction clearing utilities and acts as the cash recipient from Issuing Banks **210** and payment disburser to Merchant Bank **220**, or to Merchant **290**, if it is also acting as the Merchant Bank.

A preferred high-level view of the software components of the system of the present invention is show in Fig. 3. As shown, all parties to the system may

communicate over the Internet through their respective client software components. Account Holder **280** communicates through the Account Holder client software, typically a Netscape Navigator or Microsoft Explorer Browser plug-in **380**. A Merchant **290** uses its own Merchant Transaction systems to communicate through the Merchant client software **390**, which may consist of an Authorized Merchant Application and API. The Merchant client software **390** may be integrated with the Merchant's own sales and order fulfillment systems. Issuing bank **210** communicates through Issuing Bank software **310**, which may include Issuing Bank Web Connection Module and API. Like the Merchant client software, the Issuing Bank client software is integrated into the Issuing Bank's own system. Shipper **260** communicates through Authorized Shipping Agent client software **360**, which may include an Authorized Shipper Application API. Finally, TA **250** communicates through the Account and Transaction Management Application **350**. The Account and Transaction Management Application **350** performs all of the TA functions, such as transaction term matching, account management, order fulfillment management, and the like.

Although not shown in Fig. 3, the transaction parties do not have to be connected to the system through their respective software components over the Internet, or any other public network. Other modes of communication can be considered for each of the various connections shown.

The preferred connectivity of the system of the present invention is shown in Fig. 4. Account Holder connections in the system are preferably Secured Server Links (SSLs). As shown, connection **410** between an Account Holder and a Merchant, connection **420** between an Account Holder and an Issuing Bank, and connection **430** between an Account Holder and the TA are Secured Server Links. Connection **450** between an Issuing Bank and the TA, and connection **460** between a Merchant and the TA are preferably either a Virtual Private Network Connection (VPN) or a Secure Shell Connection (SSC).

The basic process of the system of the present invention is shown in Fig. 5. At step **510**, a first transaction party sends his transaction information to the TA. At step **530**, a second transaction party sends his transaction information to the TA. At step **550**, the TA compares these transaction information packets to determine if they are identical. If they match, then the TA returns a transaction authorization at step **570**.

If they do not match, a return to start may occur or termination of the process may occur.

The basic process outlined in Fig. 5 can be achieved through many different methodologies. Two preferred embodiments are shown in Figs. 6 and 7.

A first preferred embodiment of the invention is illustrated in Figs 6A and 7A. A transaction process begins with the Account Holder **280**. As shown in Fig. 7A, Account Holder **280** visits Merchant's Website **290**, and makes purchase selections. Account Holder **280** then sends a purchase request **711** to Merchant **290** selecting the system of the present invention as the method of payment. For example, this can occur after he fills his electronic shopping cart or when he selects the Merchant's "Purchase Now" option. The purchase request typically contains such information as item Universal Price Codes (UPCs), price, and quantity.

The client software at the Merchant's Website **290** responds to the purchase request by first generating a transaction identifier (ID), then transmitting this transaction ID along with the Merchant ID and transaction information **712** to the client software on the Account Holder's computer **280**. The transaction ID is used throughout the process to identify this particular transaction. Because one buyer and one merchant may have a number of transactions over time, the transaction ID is needed to uniquely identify this particular transaction.

After the transaction information including Transaction ID and Merchant ID is transmitted to the Account Holder's computer, the Account Holder client software on the Account Holder's computer adds the Account Holder's unique ID to the information and transmits all of the information **713** to the TA **250**. For added security, the Account Holder's ID may be encrypted before it is transmitted with the rest of the transaction information. The information that is sent to TA **250** in data packet **713** defines the transaction as the Account Holder "knows" it. It is actually the client software on the Account Holder's computer that knows all of the terms of the transaction, not the actual Account Holder, as the user of the software never sees any of the identifiers used in the system. Because the Account Holder ID is only now transmitted, the Merchant is never in possession of any Account Holder information.

Upon receiving data packet **713**, TA creates and transmits an Issuing Bank approval request **720** to Issuing Bank **210** for the amount of the transaction. The client software on the Issuing Bank's system **210** uses the Account Holder's ID to

access the Account Holder's account to determine whether to approve or reject the amount requested. The Issuing Bank **210** then transmits the transaction approval code **721** to TA **250**. If the Issuing Bank **210** approves the transaction, TA **250** generates and transmits a Transaction Key **731** along with the Transaction ID to the Account Holder's computer.

Upon receipt of the transaction key, the client software on the Account Holder's computer **280** sends the Transaction key and Transaction ID to Merchant **290** in data packet **732**. In addition, the Account Holder may be prompted at this time for delivery method instructions. Delivery information will also be passed to the Merchant **290** in data packet **732**. The client software on the Merchant's system **290** then transmits the Transaction ID, Transaction key, and transaction information including delivery instructions in data packet **733** to TA **250**.

TA **250** then matches keys and associated information that was sent by the Merchant **290**. If the information matches, then TA **250** transmits an Approval Code with the Transaction ID **770** to the Merchant **290**. In addition, TA **250** transmits a debit notice **780** to Issuing Bank **210**. Upon receipt of the debit notice, Issuing Bank **210** debits Account Holder's account and credits TA's master account. The Merchant's account at the Merchant Bank or with the TA is then credited.

Finally, Merchant **290** confirms to Account Holder **280** that the transaction is complete **790**, and ships the goods.

The process for this embodiment is shown in Fig. 6A. Step **510** from Fig. 5 is expanded to include substeps **611, 612,** and **613**. At step **611**, a first transaction party sends a transaction request to the second transaction party. Step **611** corresponds to data packet **711** in Fig. 7A, where the buyer makes a purchase request from a Merchant. At step **612**, the second party sends the transaction information including his identifier to the first party. Step **612** corresponds to data packet **712** in Fig. 7A, where the Merchant transmits the Merchant ID, Transaction ID, and all of the transaction information to the buyer. At step **613**, the first party transmits all of the information he received from the second party, including the second party's identifier, and his private identifier to the TA. Step **613** corresponds to data packet **713** in Fig. 7A, where the client software on the Account Holder's computer encrypts the Account Holder's private identifier, and sends it with the transaction information received from the Merchant to the TA.

Substeps **611**, **612**, and **613** correspond to Step **510**, where a first transaction party sends the transaction terms as he knows them to the TA. In this embodiment, the first transaction party is the buyer, who is sending all of the specific purchase information, the Merchant's ID, and the Account Holder's ID to the TA. The client software on the Account Holder's machine manages all of the transmittals. The Account Holder does not have to manually transmit all of this information, and need not know what the client software is doing. The Account Holder simply makes a purchase request from the Merchant's Website. The client software on the Account Holder's computer receives the information from the Merchant, encrypts the Account Holder's ID and transmits the necessary information on to the TA.

Step **620** in Fig. 6A corresponds to data packets **720** and **721** in Fig. 7A. At step **620**, the TA makes a transaction approval request from the Issuing Bank for the Account Holder for the amount of this specific transaction, and receives the Issuing Bank's approval code. If the transaction is approved, then the process in Fig. 6A continues to step **631**.

Step **530** from Fig. 5 is expanded to include substeps **631**, **632**, and **633** in Fig. 6A. At step **631**, the TA generates and sends a Transaction Key with the Transaction ID to the client software on the Account Holder's computer. Step **631** corresponds to data packet **731** in Fig. 7A. At step **632**, the first party sends the transaction key and transaction ID the second party. Step **632** corresponds to data packet **732** in Fig. 7A. At step **633**, the second party transmits all of the information he received from the first party, including the transaction key to the TA. Step **633** corresponds to data packet **733** in Fig. 7A.

None of the substeps **631**, **632**, and **633** are apparent to a user of the system. The client software on the Account Holder's and the Merchant's computers handle all the necessary transmissions. Substeps **631**, **632**, and **633** combined result in Step **530**.

At step **550**, the TA compares all of the transaction information received from the first party in step **613** to the transaction information received from the second party in step **633** to ensure that every term, including party identifiers, matches. In addition, the TA compares the transaction key received from the second party at step **633** with the transaction key it generated and sent to the first party at step **631** to ensure a match. Only if all of the data items match does the TA send an approval code to the second party at step **570**.

In the preferred embodiment, the second party cannot complete the transaction without the transaction key. The only way that the second party can acquire the transaction key is through the first party. This protects the first party from unauthorized purchases on his account.

A second preferred embodiment of the invention is shown in Figs. 6B and 7B. In this embodiment, all communication to the TA is through one party. In this embodiment, the first party performs the same steps **611**, **612**, and **613**, transmitting the transaction terms to the TA. However, the TA receives the second party's transaction terms through the first party instead of through the TA.

As shown in Fig. 7B, a transaction process begins when Account Holder **280** visits Merchant's Website **290**, and makes purchase selections. Account Holder **280** then sends a purchase request **711** to Merchant **290** selecting the system of the present invention as the method of payment.

The client software at the Merchant's Website **290** responds to the purchase request by first generating a transaction identifier (ID), then transmitting this transaction ID along with the Merchant ID and transaction information **712** to the client software on the Account Holder's computer **280**.

After the transaction information including Transaction ID and Merchant ID is transmitted to the Account Holder's computer, the Account Holder client software on the Account Holder's computer adds the Account Holder's unique ID to the information and transmits all of the information **713** to the TA **250**.

Upon receiving data packet **713**, TA creates and transmits an Issuing Bank approval request **720** to Issuing Bank **210** for the amount of the transaction. The Issuing Bank **210** then transmits the transaction approval code **721** to TA **250**. If the Issuing Bank **210** approves the transaction, TA **250** transmits a Transaction Key **731** along with the Transaction ID to the Account Holder's computer.

Upon receipt of the transaction key, the client software on the Account Holder's computer **280** sends the Transaction key and Transaction ID to Merchant **290** in data packet **732**. In addition, the Account Holder may be prompted at this time for delivery method instructions. Delivery information will also be passed to the Merchant **290** in data packet **732**. The client software on the Merchant's system **290** will then re-transmit the Transaction ID, Transaction key, and transaction information including delivery instructions in data packet **733** back to the Account Holder **280**.

The client software on the Account Holder's computer **280** then re-transmits this information in data packet **734** to TA **250**.

TA **250** then matches keys and associated information that was sent by Account Holder **280**. If the information matches, then TA **250** transmits a Transaction Approval Code with the Transaction ID **770** to Account Holder **280**. The client software on the Account Holder's computer **280** then re-transmits the same information in data packet **771** to Merchant **290**.

In addition, TA **250** transmits a debit notice **780** to Issuing Bank **210**. Upon receipt of the debit notice, Issuing Bank **210** debits Account Holder's account and credits TA's master account. The Merchant's account at the Merchant Bank or with the TA is then credited.

Finally, Merchant **290** confirms to Account Holder **280** that the transaction is complete **790**, and ships the goods.

The process for this embodiment is shown in Fig. 6B. Step **510** from Fig. 5 is expanded to include substeps **611, 612,** and **613**. At step **611**, a first transaction party sends a transaction request to the second transaction party. Step **611** corresponds to data packet **711** in Fig. 7B, where the buyer makes a purchase request from a Merchant. At step **612**, the second party sends the transaction information including his identifier to the first party. Step **612** corresponds to data packet **712** in Fig. 7B, where the Merchant transmits the Merchant ID, Transaction ID and all of the transaction information to the buyer. At step **613**, the first party transmits all of the information he received from the second party, including the second party's identifier, and his private identifier to the TA. Step **613** corresponds to data packet **713** in Fig. 7B, where the client software on the Account Holder's computer encrypts the Account Holder's private identifier, and sends it with the transaction information.

After performing steps **611, 612,** and **613**, thereby transmitting the first party's transaction terms to the TA, the TA gets credit approval for the transaction at step **620**. After receiving approval for the transaction, the TA generates and sends a transaction key to the first party at step **631**. The first party sends the transaction key to the second party at step **632**. The second party transmits the transaction key and transaction information back to the first party at step **635**. The first party resends this transmission to the TA at step **636**. Steps **636** and **637** correspond to data packets **736** and **737** in Fig. 7B.

The TA uses the information received at step **636** to compare against the information received at step **613** and the transaction key it generated at step **631** to ensure that all terms match. Only if all of the data items match does the TA send an approval code to the first party at step **670**. The first party then retransmits the approval code to the Merchant at step **671**. Steps **670** and **671** correspond to data packets **770** and **771** in Fig. 7B.

In this second embodiment, the Merchant does not communicate directly with the TA. Instead, the Merchant transmits all of his transaction information through the Account Holder. The transmissions are not apparent to the user at the Account Holder's computer.

In the first embodiment, the TA receives the transaction key directly from the second party, and in the second embodiment, the TA receives the transaction key indirectly through the first party. However, in both embodiments, the second party cannot complete the transaction without the transaction key.

A feature of the system of the present invention is that an Account Holder does not have to use his machine or device that has the Account Holder client software installed. In the case where the Account Holder is using a "remote" computer or device that does not have the Account Holder client software installed, he may still request to use his account with the system as his method of payment.

The transaction process for a purchase made from a remote terminal is shown in Fig. 8. Steps **510** and **530** from Fig. 5 are expanded to include substeps required for a remote transaction. In this type of transaction, the Account Holder is using a computer or other electronic device that is not his "home" computer, or any computer that does not have the Account Holder client software installed on it.

As shown in step **811**, the Account Holder visits the Merchant's Website on this remote computer and makes a purchase request, selecting the system of the present invention as the method of payment. At step **813**, the Merchant client software sends the Merchant ID and transaction information to the computer that sent the purchase request to the Merchant. If there is some type of communication failure, the computer will not respond. This could happen because the Account Holder is using a computer that does not have the client software installed, for example. Therefore at step **815**, the client software on the Merchant system will not get a response, and will therefore proceed to step **817**. If the Merchant client software had

gotten a response, then this would be a standard on-line transaction and one of the methods from Fig. 6 would be used. At step **817**, the Merchant client software switches the Webpage on the Account Holder's remote computer to a remote transaction screen, and transmits the same transaction information as in step **813** to the TA's remote transaction site.

The TA connects to the Account Holder's remote server site through a SSL connection, and at step **831** requests the user to verify the transaction and answer or ask one of the security questions that the Account Holder entered when the Account was set up. The user verifies the transaction by correctly answering or asking security questions at step **833**.

At step **840**, the TA transmits a credit approval request to the Issuing Bank for the Account Holder in question for the transaction amount. The Issuing Bank approves or disapproves the amount requested by transmitting an Issuing Bank approval code or disapproval code to the TA. The TA may also request the Account Holder to select one of his stored delivery address(es) or enter a new delivery address at this point.

If the Account Holder verified the transaction in steps **831** and **833**, then the terms do "match" for purposes of step **550**. The TA can then send a transaction approval code to the Merchant along with the delivery instructions in step **871**. Although not shown, the TA transmits a debit notice to the Issuing Bank. Upon receipt of the debit notice, the Issuing Bank debits the Account Holder's account and credits TA's master account. The Merchant's account at the Merchant Bank is then credited.

At this point the remote transaction site switches the Account Holder back to the Merchant's site where the Merchant confirms to the Account Holder that the transaction is complete and will be shipped. At step **873**, the TA transmits an e-mail to the Account Holder requesting confirmation that the Account Holder completed a remote transaction. Confirmation must be received from the Account Holder within 24 hours or the transaction will be cancelled. The Account Holder may e-mail the confirmation or may call a toll-free number and answer a security question to confirm the transaction.

The system of the present invention can also handle offline transactions, such as one initiated from a telephone call. The transaction process for a purchase made

from a telephone is shown in Fig. 9. Steps **510** and **530** from Fig. 5 are expanded to include substeps preferred for this type of transaction.

As shown in step **911**, the Account Holder tells a Merchant representative that the system of the present invention as the method of payment. This is typically done over the telephone, although it can be done in person at a Merchant's store. After gathering the needed information concerning the purchase request from the customer (Account Holder), at step **913**, the Merchant transmits the Merchant ID, Transaction ID, customer name, UPCs, prices, purchase amount, and delivery instructions to the TA. The TA generates a unique off-line transaction ID for this transaction and transmits it to the Merchant at step **920**. At step **922**, the Merchant phone or in-store representative informs the Account Holder of the off-line transaction ID and preferably a toll-free number to call to complete the transaction.

At step **931**, the Account Holder preferably calls the toll-free number and enters the off-line transaction ID. Other types of communication by the Account Holder could also be considered. The TA pulls the transaction from its database and reads it to the Account Holder using voice generation technology. The Account Holder accepts or rejects the transaction at step **933**. If accepted, then the TA prompts the Account Holder to randomly select from the Account Holder's stored security questions at step **935**. These questions were set up when the Account Holder enrolled in the system of the present invention. The TA may then use text to voice conversion technology to determine whether the security questions are answered correctly.

As in the previously described methodologies, at step **940** the TA transmits a credit approval request to the Issuing Bank for the Account Holder in question for the transaction amount. The Issuing Bank approves or disapproves the amount requested by transmitting an Issuing Bank approval code or disapproval code to the TA. If the Account Holder verified the transaction in steps **933** and **935**, then the terms do "match" for purposes of step **550**. The TA can then send a transaction approval code to the Merchant in step **971**. Although not shown, the TA transmits a debit notice to the Issuing Bank. Upon receipt of the debit notice, the Issuing Bank debits the Account Holder's account and credits TA's master account. The Merchant's account at the Merchant Bank is then credited.

The system of the present invention can also reduce fraud through its Order Confirmation and Delivery Service. After the Account Holder has made his purchase

selection and the system has validated the purchase, the Account Holder may choose one of his previously stored delivery address(es) or enter a new delivery address. For example, in the first embodiment of the present invention shown in Figs 6A and 7A, this can be done as part of step **632** in data packet **732**. This delivery information becomes part of the transaction information that is transmitted to the TA in step **633** as part of data packet **733**. When the TA performs the match in step **550**, the delivery information is part of the information compared to determine whether the transaction is valid.

The information flow for the Order Confirmation and Delivery process is shown in Fig. 10. After Merchant **290** sends a sale completed confirmation notice **790** to Account Holder **280** (as shown in Figs 7A and 7B), Merchant **290** transfers packaged goods to Shipper **260** with delivery instructions **1010**. Shipper **260** then delivers the Shipper's package/shipping ID to Merchant through data packet **1020**. The Merchant then sends the transaction ID along with the shipping ID and shipping date to TA **250** as data packet **1030**.

TA **250** periodically transmits its package watch list to Shipper **260** and indicates which ones must have signatures and from whom such signatures must be obtained if it is a delivery versus payment (DVP) shipment at data packet **1040**. DVP shipments require picture identification, or some other type of physical authentication such as a thumbprint, or other biometric data.

Goods are delivered to Account Holder's **280** specified delivery address at **1050**. The required signature or biometric sample, if any, is obtained following normal retry procedures. Account Holder **280** then accepts the delivery and signs if required at **1055**.

Shipper **260** transmits Package Change Statuses to TA **250** to confirm receipt of the goods in data packet **1060**. TA **250** transmits Transaction ID and receipt status upon any change in status to Merchant **290** in data packet **1070**.

If the transaction is DVP, the Merchant's account is credited upon notice that the goods have been delivered and the authorized signature has been obtained, and TA **250** notifies Issuing Bank **210** to debit the Account Holder's account in data packet **1080**.

The system can also handle the transmission and downloading of purchased intellectual property items, such as music, news articles, and software. This use of a

network linking buyers, sellers and a transaction administrator allows for the secure sales and delivery of intellectual property data items. The linkage between the purchase and usage of intellectual property provides better management of these assets, because the purchase and delivery is managed by the same system.

The downloaded intellectual property goes to the Account Holder's computer that already has the Account Holder client software installed on it. Therefore the Account holder client software can track the delivery and usage of any such purchased and downloaded intellectual property. This link allows merchants to have a better understanding of who is actually downloading their intellectual property, whether the intellectual property is copied, and how many times it is copied or played.

In addition, financial instruments such as online mutual funds can be purchased and delivered through the system of the present invention. The system can also handle person-to-person money wires and cash advances. The system can also securely deliver a password for an online service to an account holder.

The system provides these types of electronic file and/or password delivery through a combination of public and private encryption keys. The Account Holder is the only party that ever receives the private portion of the encryption key from the TA. Merchants and other third parties may receive the public portion of the encryption key. This combination protects the downloaded files and/or password from theft and unauthorized use.

The information flow for the online delivery process is shown in Fig. 11. As shown, the Account Holder **280** makes a purchase request from Merchant **290** for an intellectual property item that is capable of electronic delivery through data packet **1111**. Merchant **290** transmits the Merchant ID, transaction ID, product description(s), price information, delivery information (including date, time and method) to the client software on the Account Holder's computer **280** in data packet **1112**.

The Account Holder client software **280** transmits the information received in packet **1112** plus the encrypted Account Holder's private ID located on the Account Holder's system to TA **250** in data packet **1113**. TA **250** transmits an Issuing Bank approval request to Issuing Bank **210** for the amount of the purchase in data packet **1120**. Issuing Bank **210** approves or disapproves the transaction through the Approval/Disapproval Code **1121**.

If the credit is approved, TA **250** transmits a transaction key, the Transaction ID and a private portion of the online delivery encryption key to the Account Holder's client software **280**. Account Holder client software **280** transmits the transaction key and Transaction ID to Merchant **290** in data packet **1132**. The private portion of the online delivery encryption key will be used to decrypt the file or information when it is electronically delivered. By using a private encryption key in this manner, the delivery of the purchased electronic goods or services is more secure.

Merchant **290** then transmits the transaction key, Merchant ID, Transaction ID and transaction information to TA **250** in data packet **1133**.

TA **250** matches the keys and associated information regarding delivery, etc. and sends a transaction approval code with the Transaction ID and the public portion of the online delivery encryption key to Merchant **290** in data packet **1170**.

Merchant **290** may then avail itself of the option to engage in a secure transaction for the intellectual property or password so that the information/product will be encrypted using the public half of the online delivery encryption key. When Account Holder **280** executes an unpack command on the downloaded file or the downloaded file automatically executes an unpack, the program will retrieve the private half of the encryption key from the Account Holder's client software by using the Transaction ID and transaction key. This private portion of the encryption key is then used to decrypt the downloaded file/password. Additionally, the unpack can set flags in the Account Holder client software for tracking the delivery and usage of the downloaded intellectual property.

When Account Holder client software **280** completes decrypting the delivered file, it sends a completion code, Transaction ID and the public portion of the online delivery encryption key to TA **250** in data packet **1174**. TA **250** sends a debit notice to Issuing Bank **210** in data packet **1180**, and Issuing Bank **210** credits the TA master account. The Merchant's Account at the Merchant Bank or with the TA is then credited on the terms in accordance with the Merchant's agreement with the system.

The system of the present invention may also be used for periodic payments. This feature may be used in sales of monthly ISP service or for an installment loan, for example. The information flow for a periodic payment purchase is shown in Fig. 12. Data packet **1132** is the same as for the embodiment shown in Fig. 11, only now the periodic price is included in the information rather than the total purchase price.

For periodic payment purchases, the Merchant receives a payment every payment period. Fig. 12 illustrates the preferred steps that are taken each payment period for a purchase on a periodic basis. In data packet **1240** Merchant **290** transmits the transaction key, transaction ID, transaction information and periodic price to TA **250**. Upon receipt of data packet **1240**, TA **250** matches the keys and associated information regarding delivery , etc. and requests Issuing Bank approval for the periodic payment in data packet **1242**. Issuing bank **210** approves or disapproves the amount requested and transmits an Issuing bank approval code **1244** to TA **250**. Issuing Bank **210** will receive and approve such a request from TA **250** once every payment period. In contrast, in a full price transaction, as shown in Fig. 11, the full purchase price is approved only once.

After the periodic payment is approved, Issuing Bank **210** debits the Account Holder's account, and credits the Merchant's account with the Merchant Bank or with TA in data packet **1280**.

An important feature of the system of the present invention is the ability to easily "unwind" a transaction. In current systems, the return process is handled manually and is therefore quite expensive. It can cost as much as $25 or $30 to process the return of purchased goods, because every party to the transaction, including the buyer, the merchant and any associated financial institutions, must manually process the return transaction. With the growth of microtransactions on the Internet, this cost is unacceptable.

However, in the system of the present invention, the TA has all of the data for every transaction that is processed through it. In addition, every party to a transaction is electronically linked to the TA. Therefore, the TA can process an unwind transaction as easily as a regular purchase transaction.

In a preferred embodiment of an unwind transaction, an Account Holder can return a product purchased through the system of the present invention by simply visiting the Merchant's Website to request a return number. The system then processes this new transaction by sending a request for pick-up to a Shipper participating in the system. The Account Holder gives the return goods to the Shipper, which is tracked by the system. The Merchant receives the return goods in due course. The TA clears the transaction, credits the Account Holder's account and

debits the Merchant's account, as it tracks the delivery of the return goods. No other intervention by any party is needed.

The system of the present invention can completely unwind a transaction with no external communication. Because the return goods were purchased through the system, the TA already has all of the information necessary for the unwind transaction

An unwind may be handled by the system of the present invention as a regular transaction, where the Account Holder is the party that is delivering goods to the Merchant. It can be handled like a regular transaction with the parties reversed.

While the invention has been described in detail and with reference to specific embodiments thereof, it will be apparent to one skilled in the art that various changes and modifications can be made therein without departing from the spirit and scope thereof. It is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method of authenticating an electronic transaction between a plurality of transaction parties, comprising the steps of:
(a) receiving the terms of the transaction from a first transaction party;
(b) receiving the terms of the transaction from a second transaction party;
(c) comparing the terms of the transaction received from the first transaction party with the terms of the transaction received from the second transaction party to determine whether the terms match; and
(d) if the terms match, validating the transaction.

2. The method of claim 1, comprising the additional step of returning the results of the validation in step (d) to a transaction party.

3. The method of claim 1, wherein step (a) comprises electronically receiving the terms of the transaction from a first transaction party.

4. The method of claim 3, wherein step (a) comprises electronically receiving the terms of the transaction from client software on a first transaction party's computer system.

5. The method of claim 1, wherein step (b) comprises electronically receiving the terms of transaction from a second transaction party.

6. The method of claim 5, wherein step (b) comprises electronically receiving the terms of the transaction from client software one second transaction party's computer system.

7. The method of claim 1, wherein the terms of the transaction received in step (a) includes the first transaction party's identifier and the second transaction party's identifier.

8. The method of claim 1, wherein the terms of the transaction received in step (b) includes the first transaction party's identifier, the second transaction party's identifier and a transaction key.

9. The method of claim 1, wherein step (a) comprises the additional step of obtaining credit approval for the transaction.

10. The method of claim 1, wherein step (a) comprises the additional step of generating and transmitting a transaction key to the first transaction party.

11. The method of claim 1, wherein the terms compared in step (c) comprises the first transaction party's identifier, the second transaction party's identifier and sales information.

12. The method of claim 1, wherein the first transaction party is a buyer and the second transaction party is a seller.

13. The method of claim 1, wherein the identifiers are generated by client software on the computer systems of the transaction parties.

14. The method of claim 1, wherein the terms of the transaction include delivery information.

15. A method for a seller to obtain authorization of an electronic transaction, comprising the steps of:
(a) providing transaction information including a seller identifier to a buyer;
(b) receiving a transaction key from the buyer;
(c) transmitting the transaction key to a transaction administrator; and
(d) receiving an authorization from the transaction administrator.

16. A method of authorizing an electronic transaction between a plurality of transaction participants by a transaction administrator, comprising the steps of:

(a) providing transaction information by a first transaction party to the transaction administrator;

(b) generating a transaction key by the transaction administrator and providing the transaction key from the transaction administrator to the first transaction party;

(c) providing the transaction key from the first transaction party to a second transaction party;

(d) providing the transaction key from a second transaction party to the transaction administrator for validation; and

(e) validating the transaction by the transaction administrator.

17. The method of claim 16, comprising the additional step of providing the results of the validation in step (e) to a transaction party.

18. The method of claim 16, wherein step (a) comprises the steps of:

(i) a first transaction party sending a transaction request to a second transaction party;

(ii) the second transaction party sending transaction information and second transaction party identifier to the first transaction party; and

(iii) the first transaction party sending transaction information, second transaction party identifier and first transaction party identifier to the transaction administrator.

19. The method of claim 16, wherein step (c) comprises the steps of :

(i) the transaction administrator sending a transaction key to the first transaction party;

(ii) the first transaction party sending the transaction key to the second transaction party; and

(iii) the second transaction party sending transaction information and the transaction key to the transaction administrator.

20. The method of claim 16, wherein step (a) comprises electronically transmitting transaction information from a first transaction party to the transaction administrator.

21. The method of claim 20, wherein step (a) comprises electronically transmitting transaction information from client software on the first transaction party's computer system to the transaction administrator.

22. The method of claim 16, wherein the transaction information includes sales information.

23. The method of claim 16, wherein the transaction information includes delivery information.

24. The method of claim 16, wherein the transaction information in step (a) includes an identifier for each transaction party.

25. The method of claim 24, wherein the identifiers are generated by client software on each transaction party's computer system.

26. The method of claim 16, wherein generating a transaction key in step (b) comprises the step of matching party identifiers.

27. The method of claim 16, wherein step (e) comprises the step of matching the transaction key received in step (d) with the transaction key generated in step (b).

28. The method of claim 16, wherein the transaction information of step (a) includes a personal identification number, and step (e) comprises the step of matching the personal identification number from step (a) with a stored personal identification number.

29. The method of claim 16, wherein step (b) comprises the additional step of obtaining credit approval for the transaction.

30. A method of authorizing an electronic transaction between a plurality of transaction participants by a transaction administrator, comprising the steps of:
(a) providing transaction information by a first transaction party to the transaction administrator;
(b) generating a transaction key by the transaction administrator and providing the transaction key from the transaction administrator to the first transaction party;
(c) providing the transaction key from the first transaction party to a second transaction party;
(d) providing the transaction key from a second transaction party to the first transaction party;
(e) providing the transaction key from the first transaction party to the transaction administrator for validation; and
(f) validating the transaction by the transaction administrator.

31. A method of authenticating the delivery of goods between a plurality of transaction parties, comprising the steps of:
(a) providing a transaction administration system for confirming delivery of purchases;
(b) receiving the terms of the delivery from a transaction party;
(c) receiving the confirmation of the delivery from a delivery agent; and
(d) comparing the terms of the delivery received from the transaction party with the delivery confirmation to determine whether the terms match.

32. A method of authenticating a transaction between a plurality of transaction parties, comprising the steps of:
(a) requesting a transaction from a second transaction party by a first transaction party;
(b) providing transaction information to the transaction administrator by the second transaction party;

(c) requesting the first transaction party to confirm the transaction request;

(d) providing confirmation to the transaction administrator by the first transaction party;

(e) comparing the confirmation with stored confirmation data for the first transaction party; and

(f) validating the transaction by the transaction administrator.

33. A method of authenticating a transaction between a plurality of transaction parties, comprising the steps of:

(a) requesting a transaction by a first transaction party from a second transaction party;

(b) providing transaction information to the transaction administrator from the second transaction party;

(c) providing a transaction number to the second transaction party by the transaction administrator;

(d) communicating the transaction number to the first transaction party by the second transaction party;

(e) confirming the transaction by the first transaction party contacting the transaction administrator and communicating the transaction number;

(f) comparing the confirmation provided by the first transaction party with the stored transaction number; and

(g) validating the transaction by the transaction administrator.

34. A method of unwinding a transaction between a buyer and a seller each having an account with a transaction administrator, comprising the steps of:

(a) requesting a return transaction from the seller;

(b) receiving a return transaction number;

(c) returning goods to a delivery agent;

(d) delivering the return goods to the seller by the delivery agent; and

(e) crediting the buyer's account and debiting the merchant's account by the transaction administrator upon the seller's receipt of the return goods.

35. A method of verifying the electronic purchase and delivery of intellectual property between a plurality of transaction parties, where a first transaction party requests to purchase downloadable intellectual property from a second transaction party by a transaction administrator, comprising the steps of:

(a) providing transaction information to a transaction administrator;

(b) generating and providing a transaction key and a private delivery key to the first transaction party by the transaction administrator;

(c) providing the transaction key to the second transaction party from the first transaction party;

(d) providing the transaction key to the transaction administrator by the second transaction party;

(e) validating the transaction by comparing the received transaction key with the one generated;

(f) if the transaction is validated, providing a public delivery key to the second transaction party;

(g) providing the intellectual property to the first transaction party encrypted with the private delivery key; and

(h) decrypting the intellectual property by the first transaction party.

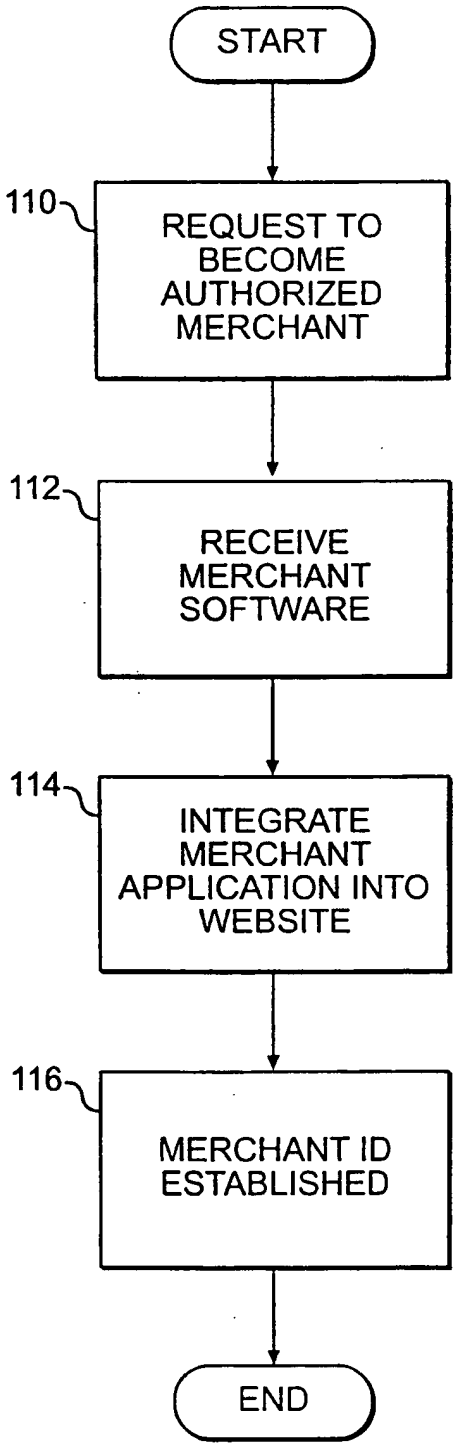
START
110
REQUEST TO BECOME AUTHORIZED MERCHANT
112
RECEIVE MERCHANT SOFTWARE
114
INTEGRATE MERCHANT APPLICATION INTO WEBSITE
116
MERCHANT ID ESTABLISHED
END

FIG. 1A

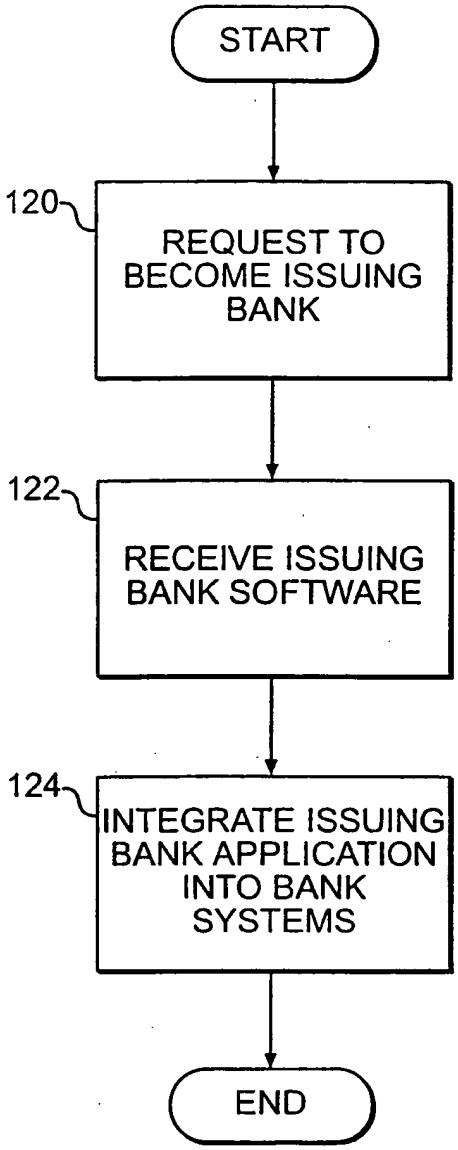
START
120
REQUEST TO BECOME ISSUING BANK
122
RECEIVE ISSUING BANK SOFTWARE
124
INTEGRATE ISSUING BANK APPLICATION INTO BANK SYSTEMS
END

FIG. 1B

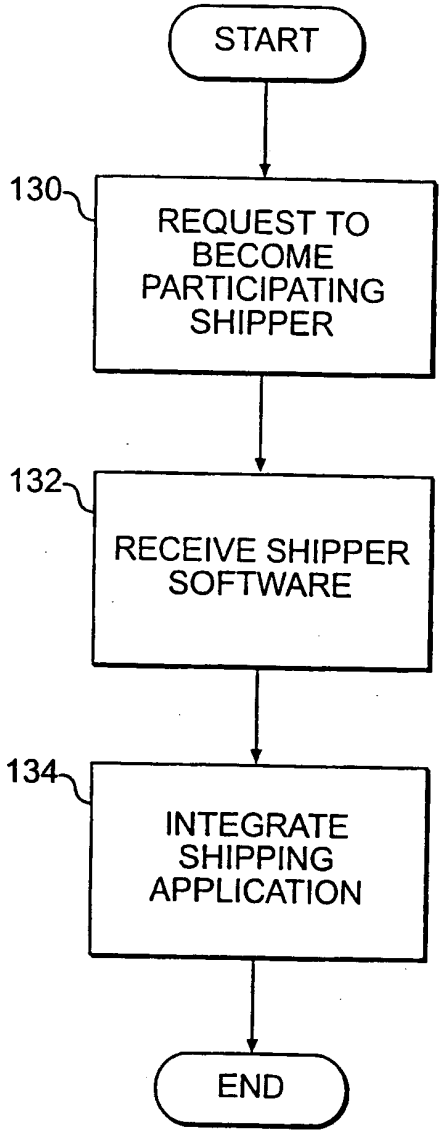
START
130
REQUEST TO BECOME PARTICIPATING SHIPPER
132
RECEIVE SHIPPER SOFTWARE
134
INTEGRATE SHIPPING APPLICATION
END

FIG. 1C

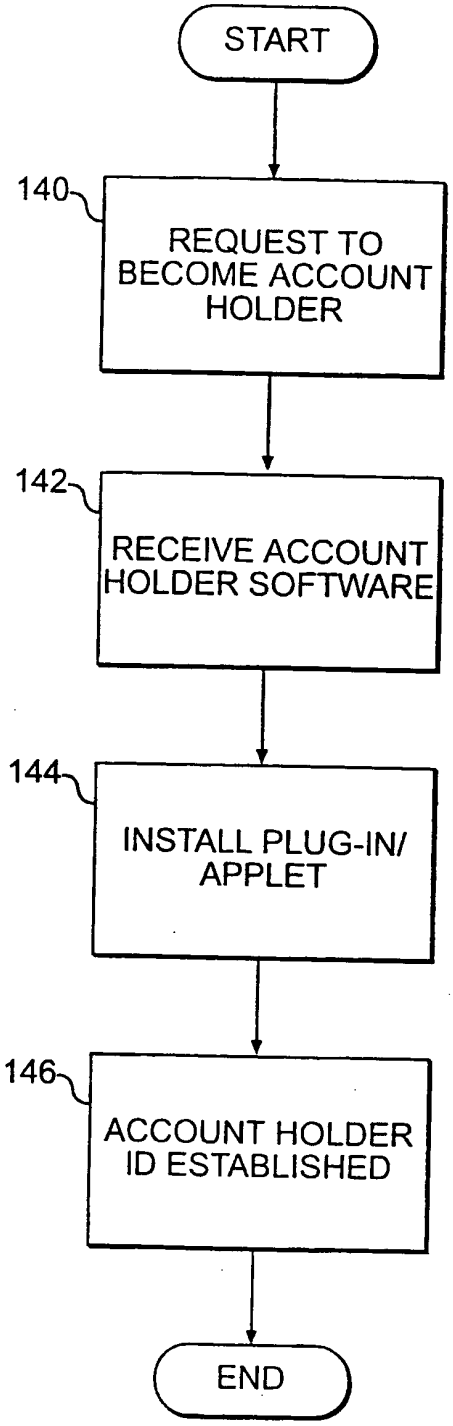
START
140
REQUEST TO BECOME ACCOUNT HOLDER
142
RECEIVE ACCOUNT HOLDER SOFTWARE
144
INSTALL PLUG-IN/ APPLET
146
ACCOUNT HOLDER ID ESTABLISHED
END

FIG. 1D

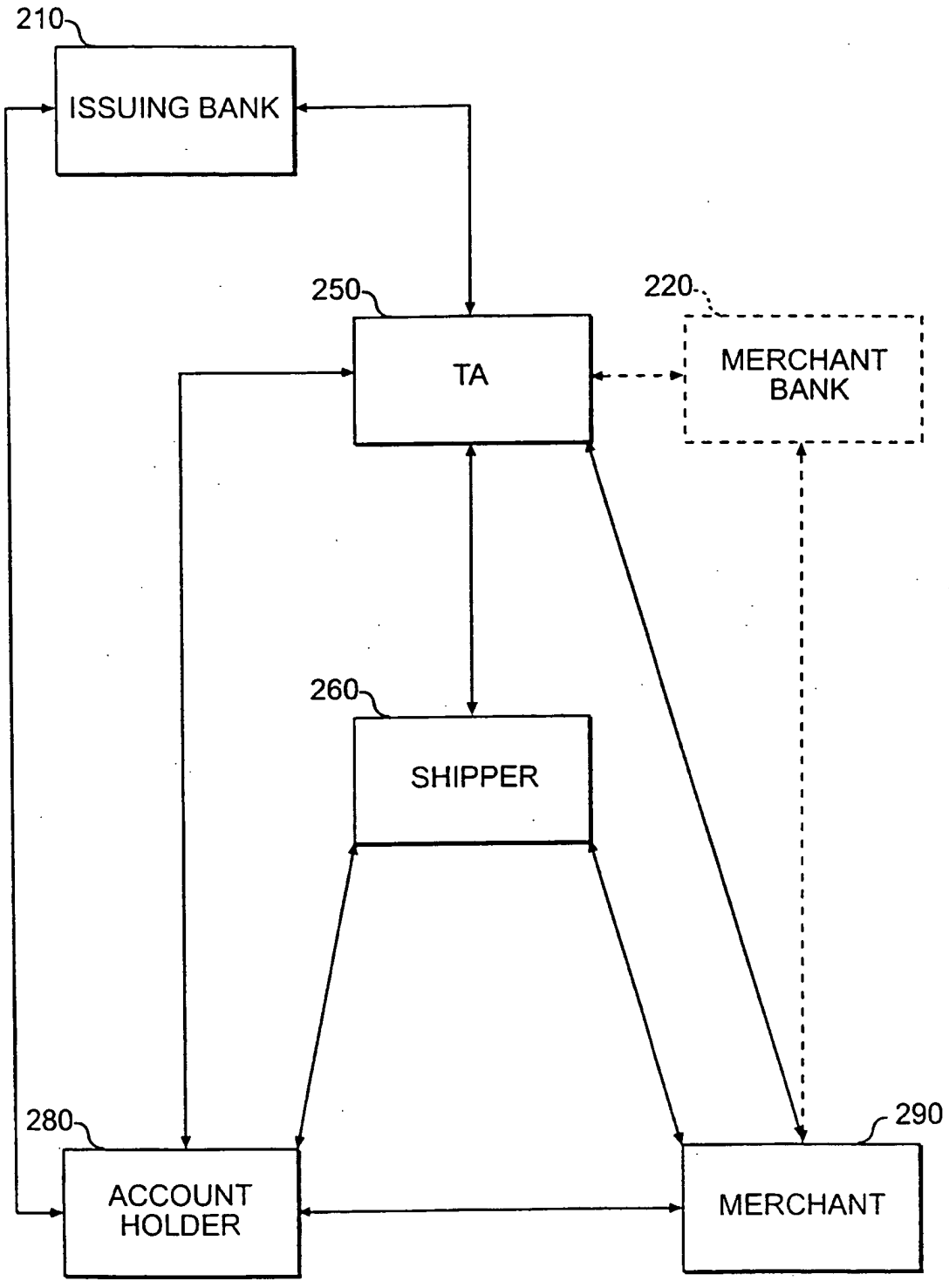
210
ISSUING BANK
250
TA
220
MERCHANT BANK
260
SHIPPER
280
ACCOUNT HOLDER
290
MERCHANT

FIG. 2

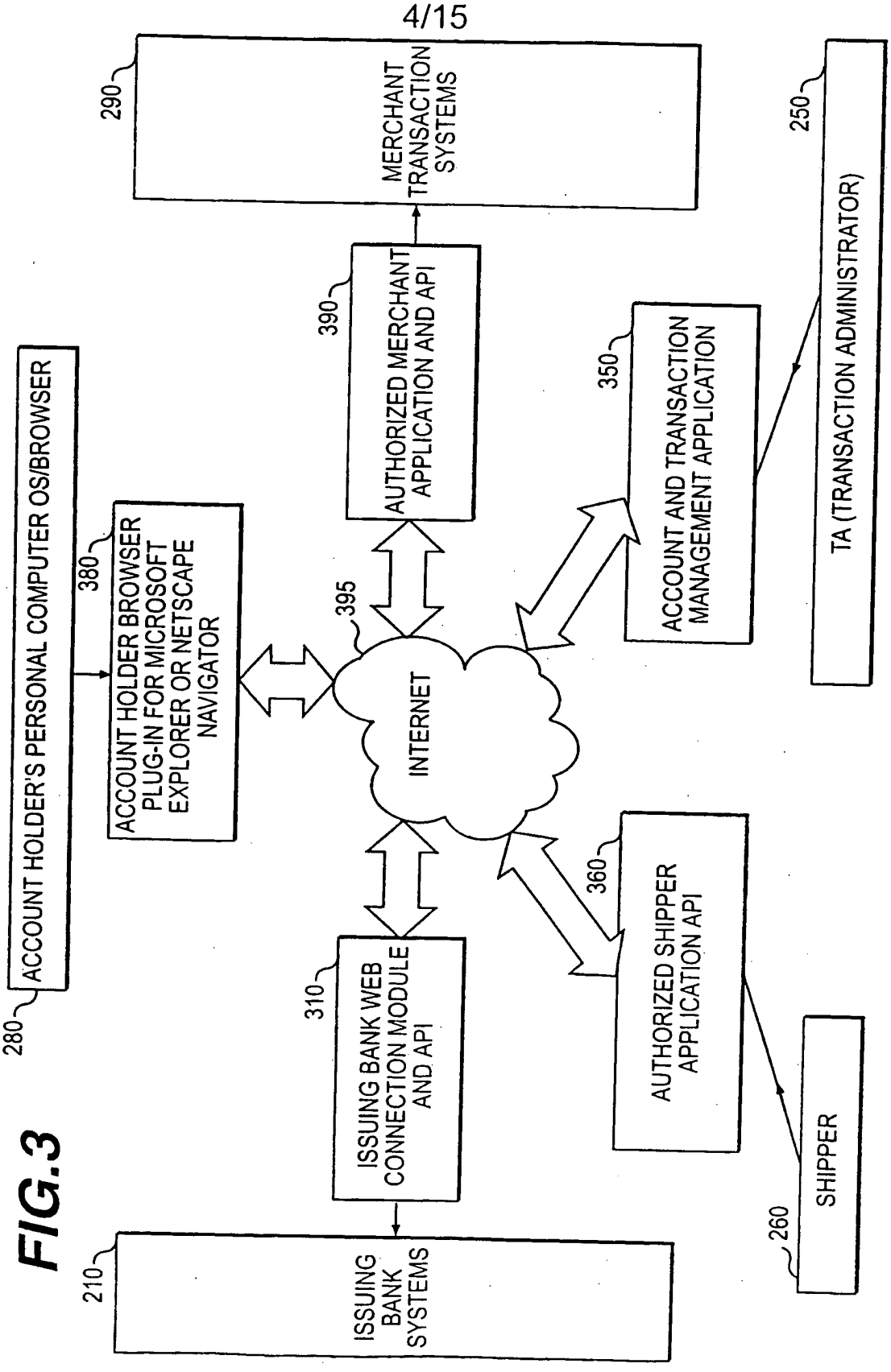
290
MERCHANT TRANSACTION SYSTEMS
250
TA (TRANSACTION ADMINISTRATOR)
390
AUTHORIZED MERCHANT APPLICATION AND API
350
ACCOUNT AND TRANSACTION MANAGEMENT APPLICATION
380
ACCOUNT HOLDER BROWSER PLUG-IN FOR MICROSOFT EXPLORER OR NETSCAPE NAVIGATOR
395
INTERNET
ACCOUNT HOLDER'S PERSONAL COMPUTER OS/BROWSER
280
360
AUTHORIZED SHIPPER APPLICATION API
310
ISSUING BANK WEB CONNECTION MODULE AND API
260
SHIPPER
210
ISSUING BANK SYSTEMS

FIG.3

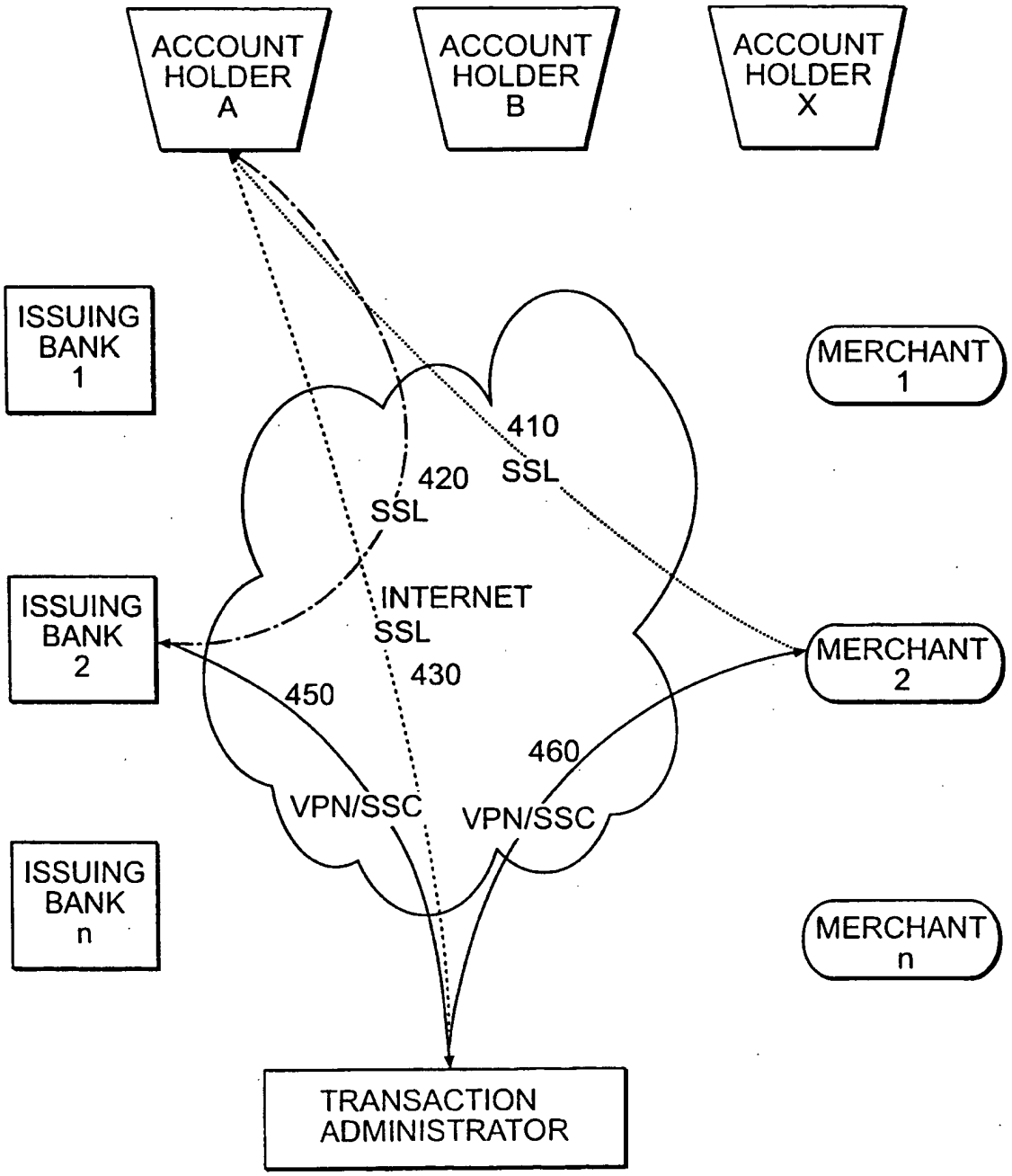
ACCOUNT HOLDER A
ACCOUNT HOLDER B
ACCOUNT HOLDER X
ISSUING BANK 1
ISSUING BANK 2
ISSUING BANK n
MERCHANT 1
MERCHANT 2
MERCHANT n
410
SSL
420
SSL
INTERNET
SSL
430
450
460
VPN/SSC
VPN/SSC
TRANSACTION ADMINISTRATOR

FIG. 4

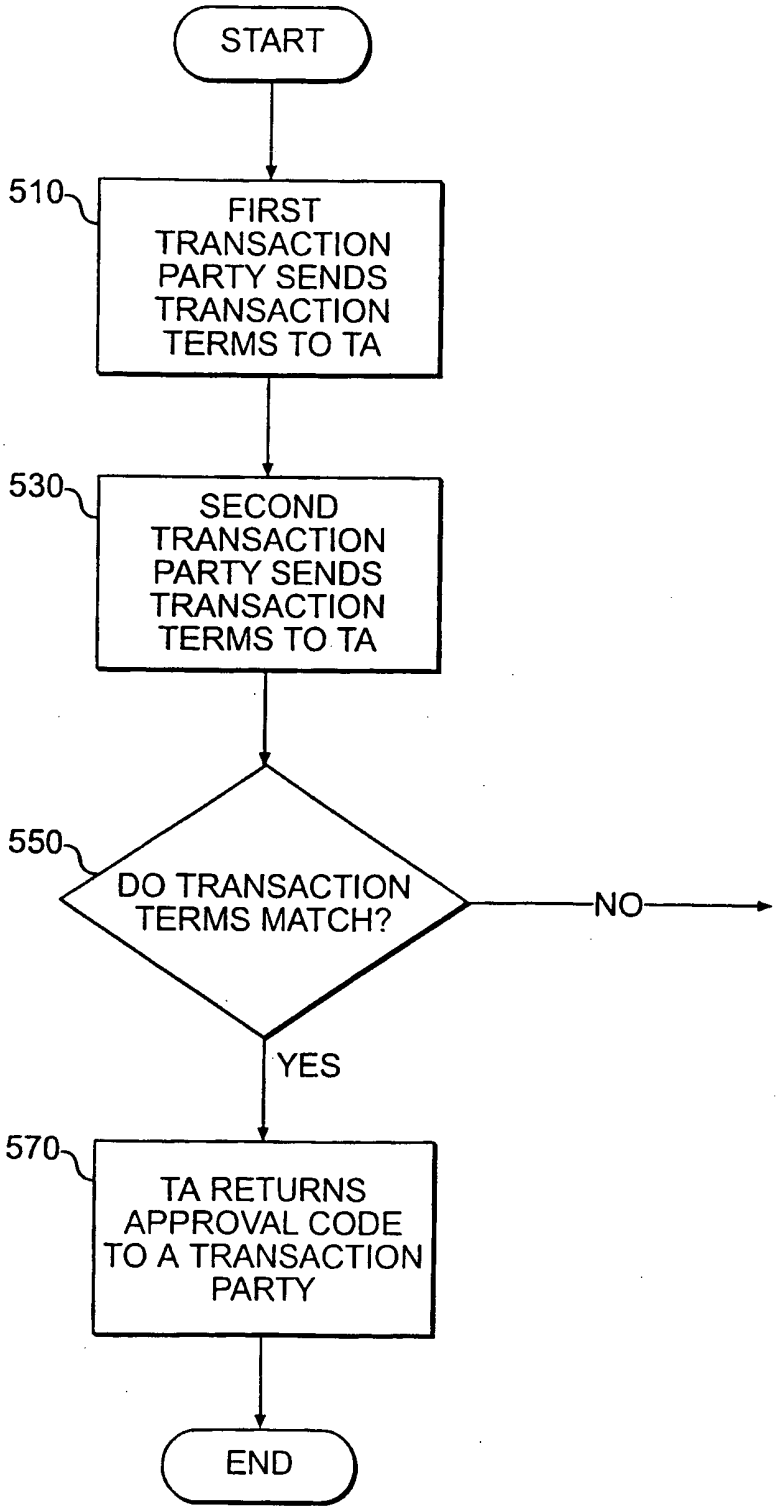
START
510
FIRST TRANSACTION PARTY SENDS TRANSACTION TERMS TO TA
530
SECOND TRANSACTION PARTY SENDS TRANSACTION TERMS TO TA
550
DO TRANSACTION TERMS MATCH?
NO
YES
570
TA RETURNS APPROVAL CODE TO A TRANSACTION PARTY
END

FIG. 5

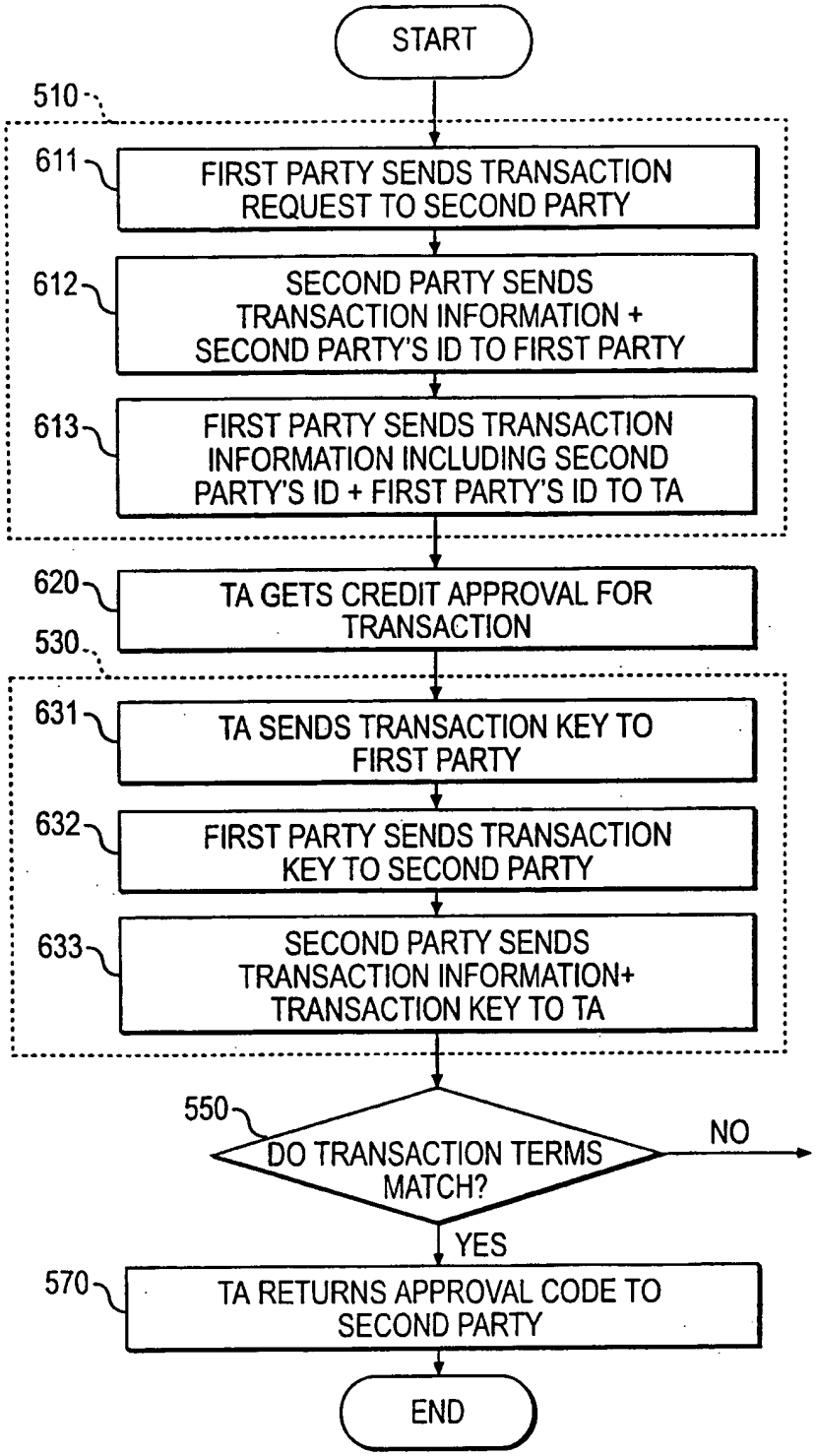
START
510
611
FIRST PARTY SENDS TRANSACTION REQUEST TO SECOND PARTY
612
SECOND PARTY SENDS TRANSACTION INFORMATION + SECOND PARTY'S ID TO FIRST PARTY
613
FIRST PARTY SENDS TRANSACTION INFORMATION INCLUDING SECOND PARTY'S ID + FIRST PARTY'S ID TO TA
620
TA GETS CREDIT APPROVAL FOR TRANSACTION
530
631
TA SENDS TRANSACTION KEY TO FIRST PARTY
632
FIRST PARTY SENDS TRANSACTION KEY TO SECOND PARTY
633
SECOND PARTY SENDS TRANSACTION INFORMATION+ TRANSACTION KEY TO TA
550
DO TRANSACTION TERMS MATCH?
NO
YES
570
TA RETURNS APPROVAL CODE TO SECOND PARTY
END

FIG. 6A

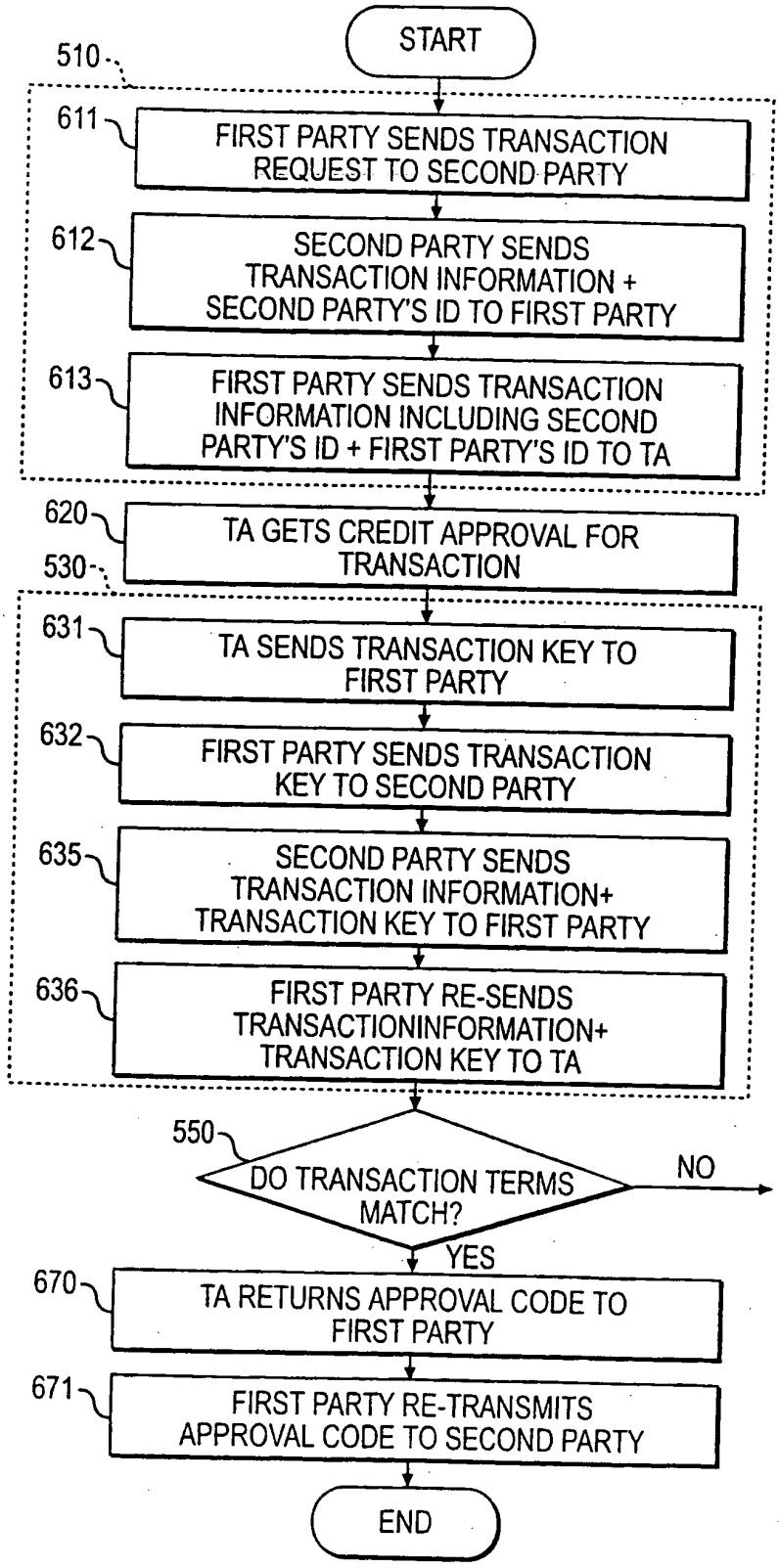
START
510
611
FIRST PARTY SENDS TRANSACTION REQUEST TO SECOND PARTY
612
SECOND PARTY SENDS TRANSACTION INFORMATION + SECOND PARTY'S ID TO FIRST PARTY
613
FIRST PARTY SENDS TRANSACTION INFORMATION INCLUDING SECOND PARTY'S ID + FIRST PARTY'S ID TO TA
620
TA GETS CREDIT APPROVAL FOR TRANSACTION
530
631
TA SENDS TRANSACTION KEY TO FIRST PARTY
632
FIRST PARTY SENDS TRANSACTION KEY TO SECOND PARTY
635
SECOND PARTY SENDS TRANSACTION INFORMATION+ TRANSACTION KEY TO FIRST PARTY
636
FIRST PARTY RE-SENDS TRANSACTIONINFORMATION+ TRANSACTION KEY TO TA
550
DO TRANSACTION TERMS MATCH?
NO
YES
670
TA RETURNS APPROVAL CODE TO FIRST PARTY
671
FIRST PARTY RE-TRANSMITS APPROVAL CODE TO SECOND PARTY
END

FIG. 6B

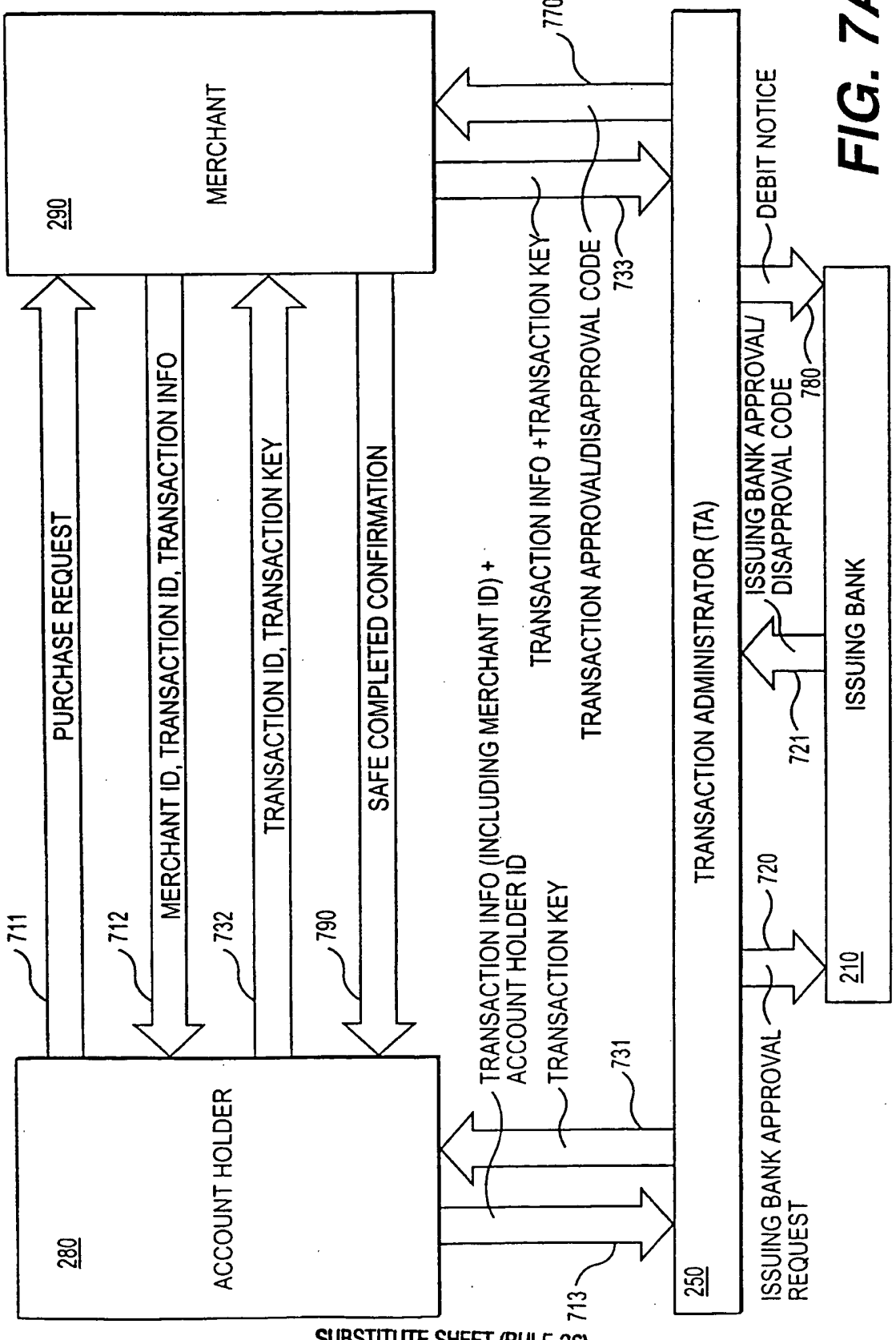
290
MERCHANT
280
ACCOUNT HOLDER
250
TRANSACTION ADMINISTRATOR (TA)
210
ISSUING BANK
PURCHASE REQUEST
MERCHANT ID, TRANSACTION ID, TRANSACTION INFO
TRANSACTION ID, TRANSACTION KEY
SAFE COMPLETED CONFIRMATION
TRANSACTION INFO (INCLUDING MERCHANT ID) + ACCOUNT HOLDER ID
TRANSACTION KEY
TRANSACTION INFO +TRANSACTION KEY
TRANSACTION APPROVAL/DISAPPROVAL CODE
ISSUING BANK APPROVAL REQUEST
ISSUING BANK APPROVAL
ISSUING BANK APPROVAL/ DISAPPROVAL CODE
DEBIT NOTICE
711
712
732
790
713
731
733
770
720
721
780

FIG. 7A

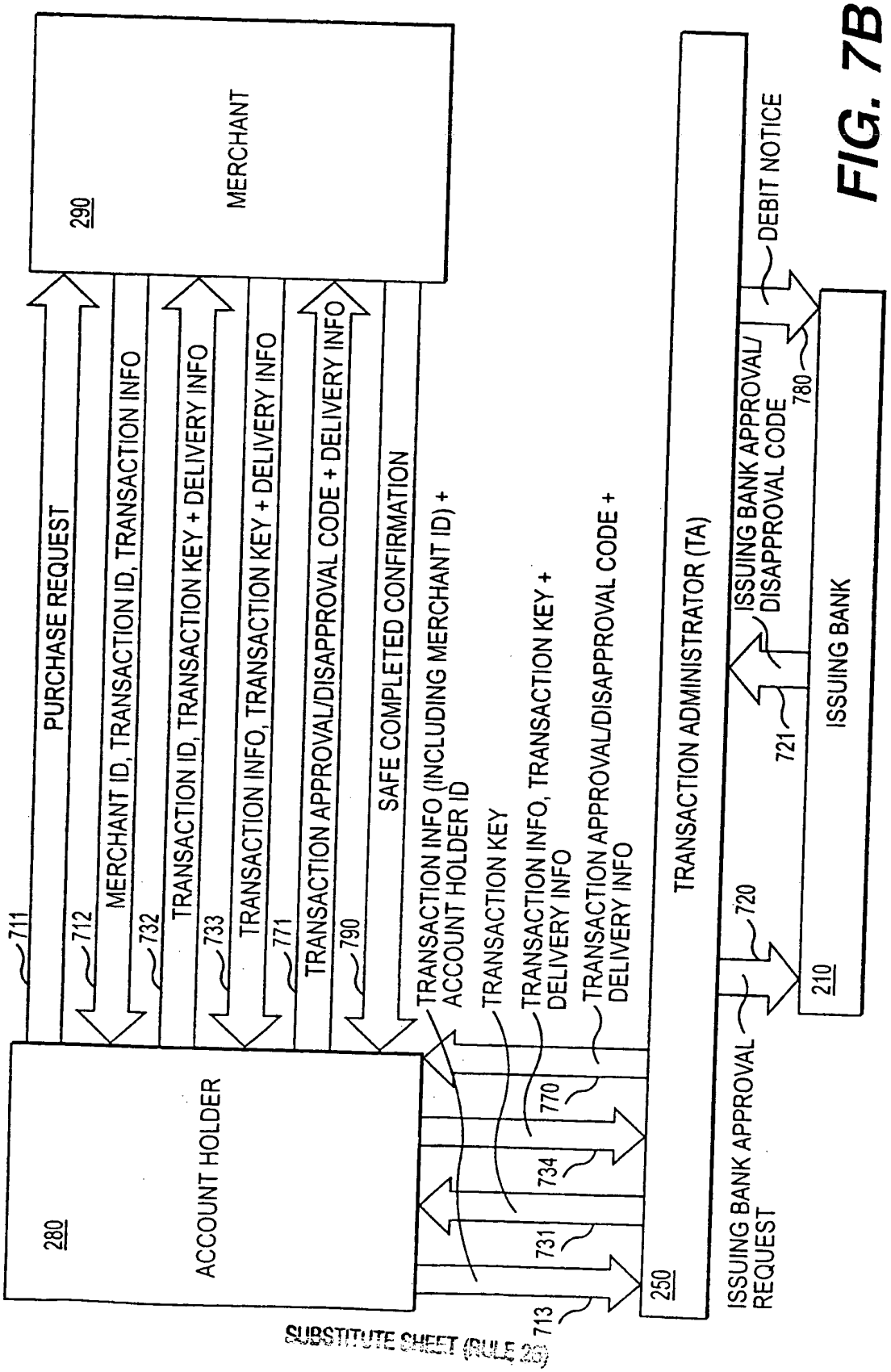
MERCHANT
290
ACCOUNT HOLDER
280
TRANSACTION ADMINISTRATOR (TA)
250
ISSUING BANK
210
PURCHASE REQUEST
711
MERCHANT ID, TRANSACTION ID, TRANSACTION INFO
712
TRANSACTION ID, TRANSACTION KEY + DELIVERY INFO
732
TRANSACTION INFO, TRANSACTION KEY + DELIVERY INFO
733
TRANSACTION APPROVAL/DISAPPROVAL CODE + DELIVERY INFO
771
SAFE COMPLETED CONFIRMATION
790
TRANSACTION INFO (INCLUDING MERCHANT ID) + ACCOUNT HOLDER ID
731
TRANSACTION KEY
734
TRANSACTION INFO, TRANSACTION KEY + DELIVERY INFO
770
TRANSACTION APPROVAL/DISAPPROVAL CODE + DELIVERY INFO
713
ISSUING BANK APPROVAL REQUEST
720
ISSUING BANK APPROVAL/ DISAPPROVAL CODE
721
DEBIT NOTICE
780

FIG. 7B

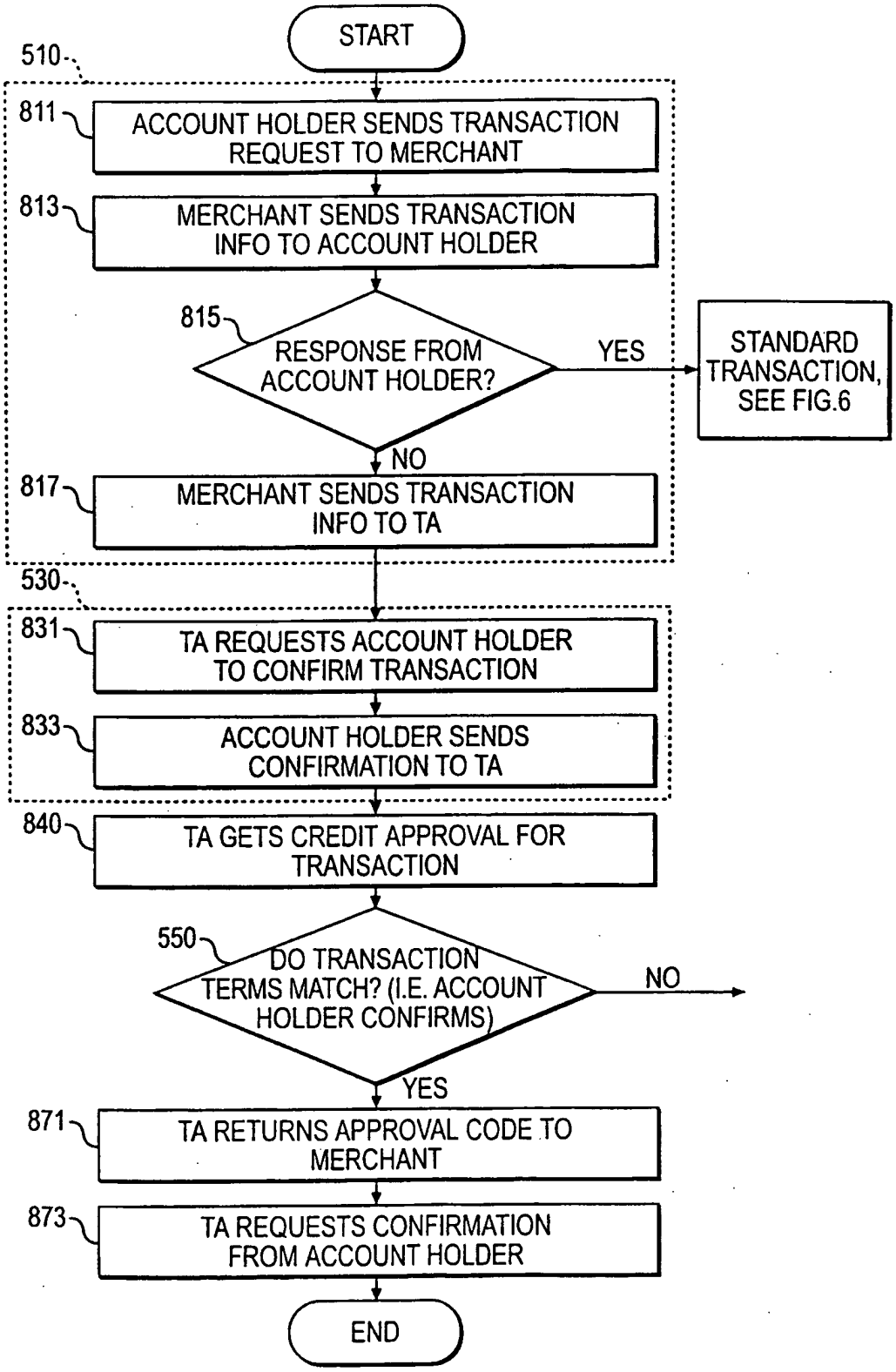
START
510
811
ACCOUNT HOLDER SENDS TRANSACTION REQUEST TO MERCHANT
813
MERCHANT SENDS TRANSACTION INFO TO ACCOUNT HOLDER
815
RESPONSE FROM ACCOUNT HOLDER?
YES
STANDARD TRANSACTION, SEE FIG.6
NO
817
MERCHANT SENDS TRANSACTION INFO TO TA
530
831
TA REQUESTS ACCOUNT HOLDER TO CONFIRM TRANSACTION
833
ACCOUNT HOLDER SENDS CONFIRMATION TO TA
840
TA GETS CREDIT APPROVAL FOR TRANSACTION
550
DO TRANSACTION TERMS MATCH? (I.E. ACCOUNT HOLDER CONFIRMS)
NO
YES
871
TA RETURNS APPROVAL CODE TO MERCHANT
873
TA REQUESTS CONFIRMATION FROM ACCOUNT HOLDER
END

FIG. 8

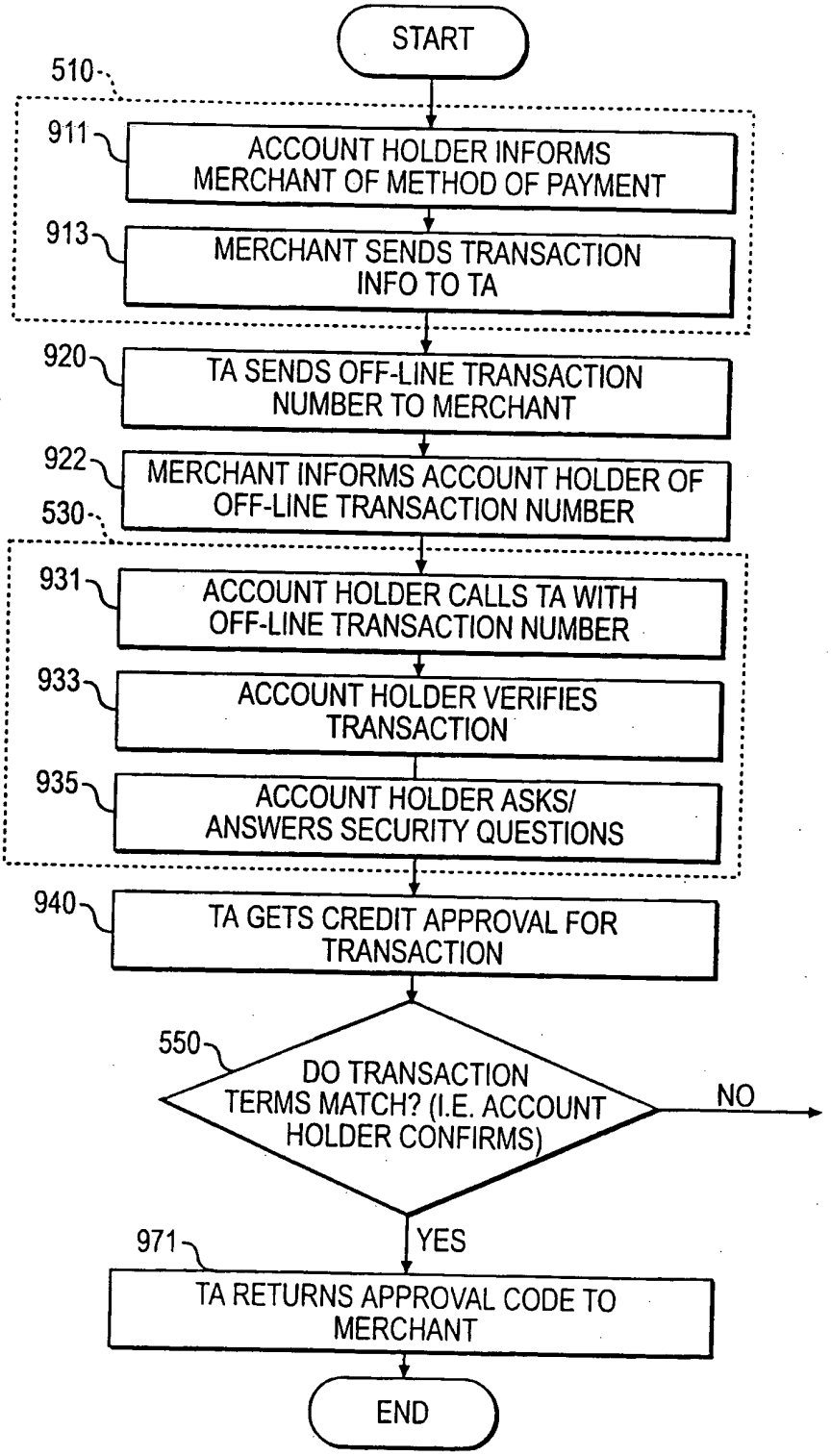
START
510
911
ACCOUNT HOLDER INFORMS MERCHANT OF METHOD OF PAYMENT
913
MERCHANT SENDS TRANSACTION INFO TO TA
920
TA SENDS OFF-LINE TRANSACTION NUMBER TO MERCHANT
922
MERCHANT INFORMS ACCOUNT HOLDER OF OFF-LINE TRANSACTION NUMBER
530
931
ACCOUNT HOLDER CALLS TA WITH OFF-LINE TRANSACTION NUMBER
933
ACCOUNT HOLDER VERIFIES TRANSACTION
935
ACCOUNT HOLDER ASKS/ ANSWERS SECURITY QUESTIONS
940
TA GETS CREDIT APPROVAL FOR TRANSACTION
550
DO TRANSACTION TERMS MATCH? (I.E. ACCOUNT HOLDER CONFIRMS)
NO
YES
971
TA RETURNS APPROVAL CODE TO MERCHANT
END

FIG. 9

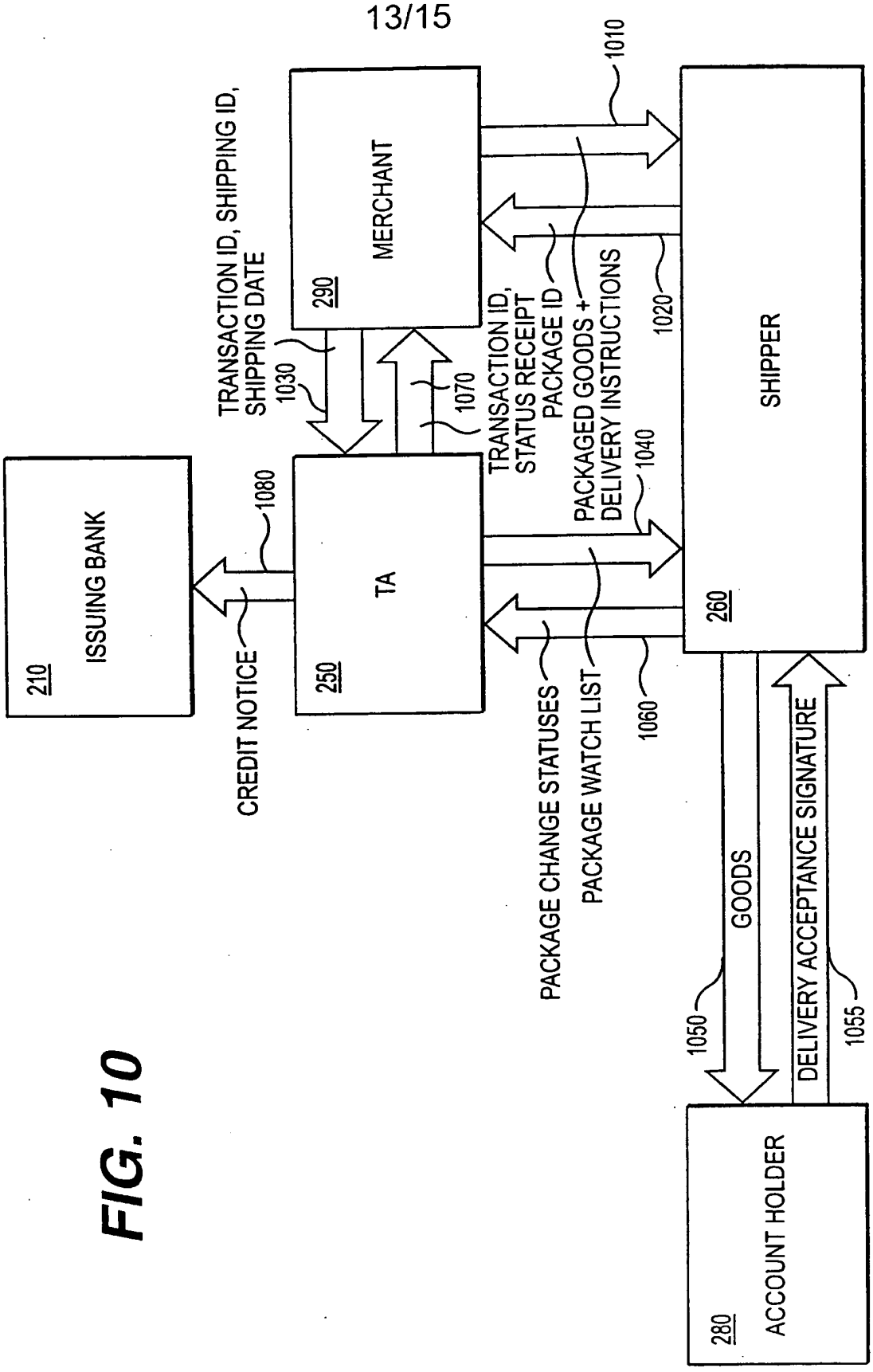
MERCHANT
290
SHIPPER
260
ISSUING BANK
210
TA
250
ACCOUNT HOLDER
280
1010
1020
1030
1040
1050
1055
1060
1070
1080
TRANSACTION ID, SHIPPING ID, SHIPPING DATE
TRANSACTION ID, STATUS RECEIPT PACKAGE ID
PACKAGED GOODS + DELIVERY INSTRUCTIONS
CREDIT NOTICE
PACKAGE CHANGE STATUSES
PACKAGE WATCH LIST
GOODS
DELIVERY ACCEPTANCE SIGNATURE

FIG. 10

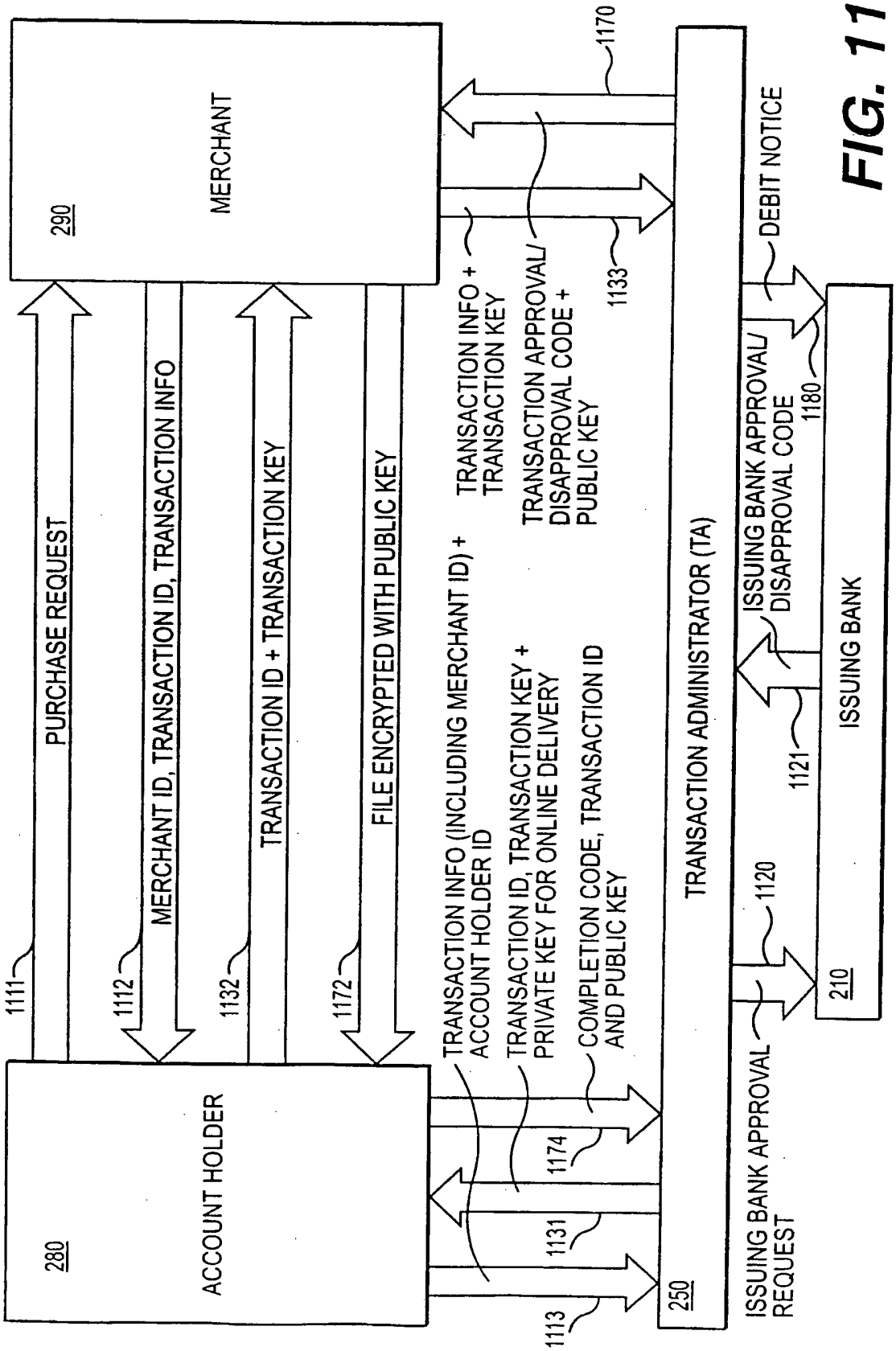
290
MERCHANT
280
ACCOUNT HOLDER
250
TRANSACTION ADMINISTRATOR (TA)
210
ISSUING BANK
PURCHASE REQUEST
MERCHANT ID, TRANSACTION ID, TRANSACTION INFO
TRANSACTION ID + TRANSACTION KEY
FILE ENCRYPTED WITH PUBLIC KEY
TRANSACTION INFO (INCLUDING MERCHANT ID) + ACCOUNT HOLDER ID
TRANSACTION ID, TRANSACTION KEY + PRIVATE KEY FOR ONLINE DELIVERY
COMPLETION CODE, TRANSACTION ID AND PUBLIC KEY
TRANSACTION INFO + TRANSACTION KEY
TRANSACTION APPROVAL/ DISAPPROVAL CODE + PUBLIC KEY
DEBIT NOTICE
ISSUING BANK APPROVAL/ DISAPPROVAL CODE
ISSUING BANK APPROVAL REQUEST
1111
1112
1132
1172
1174
1131
1113
1170
1133
1180
1121
1120

FIG. 11

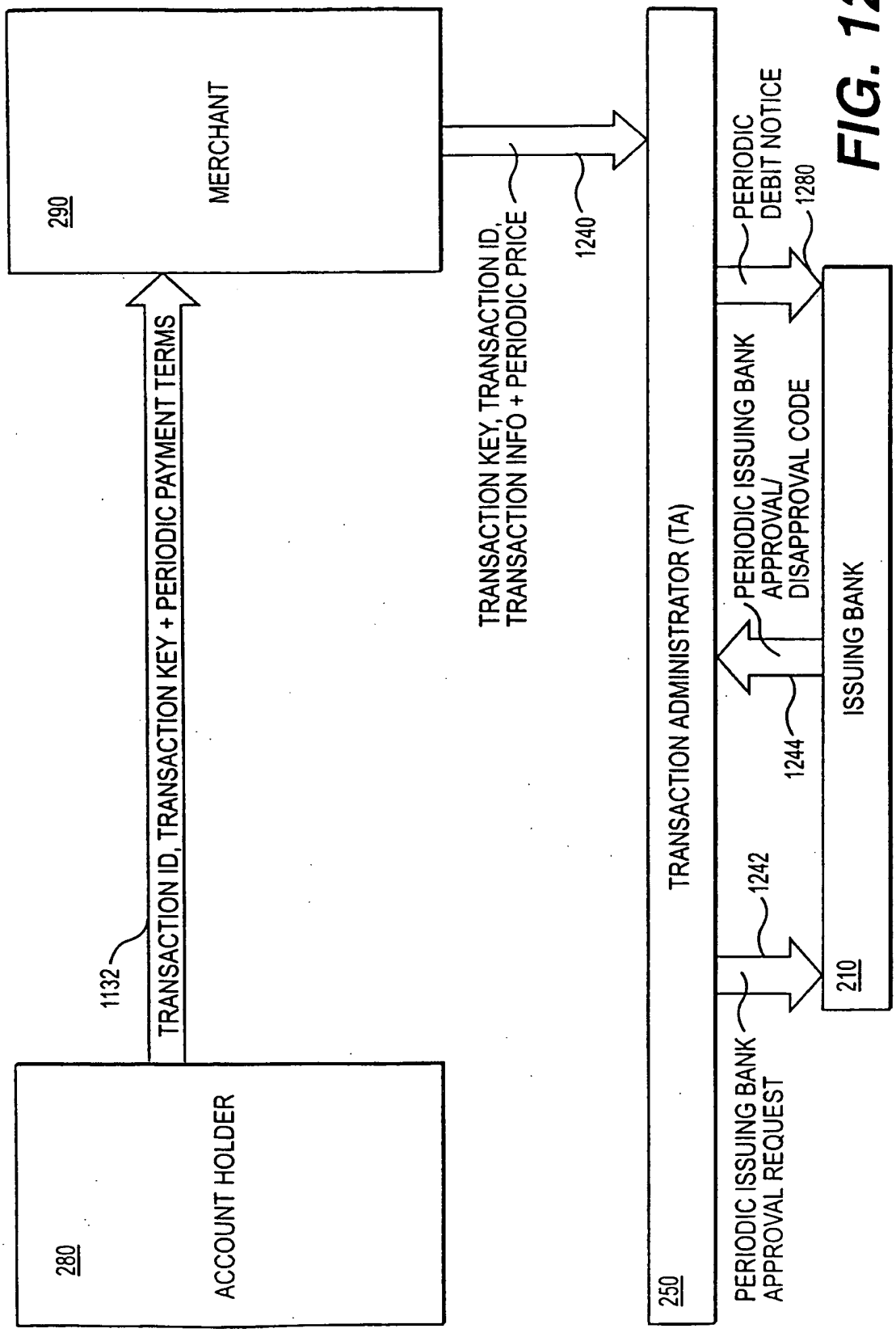
290
MERCHANT
TRANSACTION ID, TRANSACTION KEY + PERIODIC PAYMENT TERMS
1132
280
ACCOUNT HOLDER
TRANSACTION KEY, TRANSACTION ID, TRANSACTION INFO + PERIODIC PRICE
1240
PERIODIC DEBIT NOTICE
1280
TRANSACTION ADMINISTRATOR (TA)
PERIODIC ISSUING BANK APPROVAL/ DISAPPROVAL CODE
1244
ISSUING BANK
1242
210
PERIODIC ISSUING BANK APPROVAL REQUEST
250

FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/30427

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 9/00
US CL :705/64; 902/2
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/64; 902/2

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Internet-Altavista

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DIALOG, ACM Digital Library, IEEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No
X	US 5,878,143 A (MOORE) 02 March 1999, (entire document).	1-35
A, P	US 6,029,150 A (KRAVITZ) 22 February 2000, (entire document).	1-35
A	US 5,910,896 A (HAHN-CARLSON) 08 June 1999, (entire document).	1-35
A	US 4,755,940 A (BRACHTL et al.) 05 July 1988, (entire document).	1-35
A	US 4,317,957 A (SENDROW) 02 March 1982, (entire document).	1-35

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or pri date and not in conflict with the application but cited to understan principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cann considered novel or cannot be considered to involve an inventiv when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cann considered to involve an inventive step when the docum combined with one or more other such documents, such combi being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 18 DECEMBER 2000	Date of mailing of the international search report 23 FEB 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer JAMES TRAMMELL James R. Matthews Telephone No. (703) 305-3768

Form PCT/ISA/210 (second sheet) (July 1998)*